Auftragsverarbeitungsvertrag (AVV)

Stand: Oktober 2026 · Version 2.44.7

Parteien

Zwischen **Janeway.io UG (haftungsbeschränkt)**, August-Bebel-Straße 16, 16816 Neuruppin, eingetragen im Handelsregister des Amtsgericht Neuruppin unter HRB 15191 NP, vertreten durch den Geschäftsführer Lukas Pritzkow (nachfolgend „**Auftragnehmer**“)

und

Auftraggeber	
Name / Firma / Bezeichnung der Behörde	_____
Straße, Hausnummer	_____
PLZ, Ort, Land	_____
soweit vorhanden: Register und Nummer	_____
bei juristischen Personen und Personengesellschaften: vertreten durch (Name, Funktion)	_____
bei öffentlichen Stellen: vertreten durch (Name, **Amtsbezeichnung**)	_____
bei öffentlichen Stellen zusätzlich: Rechtsgrundlage der Vertretungsberechtigung	_____

(nachfolgend „**Auftraggeber**“)

— gemeinsam die „**Parteien**“ —

Dieser Auftragsverarbeitungsvertrag („**AVV**“) regelt die Verarbeitung personenbezogener Daten durch Janeway.io UG (haftungsbeschränkt) („**Auftragsverarbeiter**“) im Auftrag des Auftraggebers („**Verantwortlicher**“) gemäß Art. 28 DSGVO. **„Auftragnehmer“ ist hier der Auftragsverarbeiter; „Auftragnehmer des Verantwortlichen“ — in Ziff. 5 der Präambel und in Anlage 1 — sind dessen eigene Dienstleister.**

Datenschutzbeauftragter des Auftragsverarbeiters ist Patrick Knittel, Knittel Akademie für Datenschutz & Compliance, info@knittel-compliance.de, +49 30 5522 8166; er ist Ansprechpartner in datenschutzrechtlichen Fragen aus diesem AVV. Weisungen nach § 1 und Meldungen nach § 6 richtet der Verantwortliche an die im Abschluss benannte Kontaktstelle; Datenschutzanfragen auch an legal@janeway.io.

Präambel und Rahmenangaben

Der Verantwortliche beauftragt den Auftragsverarbeiter mit einer datenverarbeitenden Hauptleistung: (a) der cloudbasierten KI-Software-Suite (Janeway Suite) samt Modulen, (b) Betrieb, Wartung und Support von Software-Systemen (Managed Services / Hosting) oder (c) Softwareentwicklung einschließlich Testläufen mit personenbezogenen Testdaten. Sie ergibt sich aus dem Abonnement-/Nutzungsvertrag oder dem Rahmenvertrag nebst Leistungsanlagen und -scheinen (einheitlich „**Hauptvertrag**“ bzw. „**Dienste**“); Verweise auf die Janeway Suite sind beispielhaft. **Bestehen mehrere Hauptverträge nebeneinander, gilt dieser AVV für jeden gesondert:** Fristen und

Löschpflichten nach § 7 und die Haftungsobergrenze nach § 9 Abs. 2 beziehen sich auf den einzelnen Hauptvertrag und seine Vergütung; die Beendigung eines Hauptvertrags lässt die Verarbeitung unter den übrigen unberührt.

0. Abgrenzung der Rollen

(1) Erfasst sind ausschließlich Verarbeitungen, die der Auftragsverarbeiter weisungsgebunden vornimmt: die Inhalte, die der Verantwortliche oder seine Nutzer in die Anwendungen eingeben oder dort erzeugen (Ziff. 4), sowie Anlage, Verwaltung und Sicherung ihrer Konten.

(2) **Nicht Gegenstand** sind Verarbeitungen, über deren Zwecke und Mittel der Auftragsverarbeiter selbst entscheidet und für die er eigener Verantwortlicher ist (Art. 4 Nr. 7 DSGVO): Missbrauchs- und Angriffsabwehr, Abrechnung des Hauptvertrags samt Zahlungsabwicklung und Credit-Verbrauch, Betrieb der eigenen Websites samt deren Demo- und Website-Assistenten, Versand der Betriebs-, Wartungs- und Leistungsmitteilungen an die Kontaktpersonen des Verantwortlichen sowie Protokolle für eigene Pflichten nach Art. 32 DSGVO und eigene Rechtsansprüche. Insoweit gilt seine Datenschutzerklärung, Betroffenenrechte sind ihm gegenüber geltend zu machen, ein Weisungsrecht nach § 1 besteht nicht.

(3) Unterfallen dieselben Daten beiden Absätzen, entscheidet für jede Verarbeitung ihr Zweck. Eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO wird nicht begründet.

(4) **Ist der Auftraggeber für die eingebrachten Daten selbst Auftragsverarbeiter** — insbesondere, wenn er über einen Entwickler-Zugang Arbeitsbereiche, Kontingente oder Agenten für **eigene Kunden** betreibt —, verarbeitet der Auftragsverarbeiter sie als **Unterauftragsverarbeiter** nach Art. 28 Abs. 4 DSGVO. Dieser Vertrag gilt dann entsprechend; der Auftraggeber tritt an die Stelle des Verantwortlichen, über ihn verlaufen Weisungskette und Betroffenenrechte.

a) **Genehmigung.** Der Auftraggeber sichert zu, dass sein Verantwortlicher ihm die Genehmigung nach Art. 28 Abs. 2 DSGVO erteilt hat — **für den Auftragsverarbeiter wie für die in Anlage 3 geführten Empfänger**. Mitteilungen nach § 4 Abs. 2 gibt er unverzüglich weiter, damit die Einspruchsfrist nach § 4 Abs. 3 laufen kann.

b) **Durchreichen der Pflichten.** Dem weiteren Auftragsverarbeiter sind nach Art. 28 Abs. 4 DSGVO **dieselben** Pflichten aufzuerlegen, die zwischen dem Verantwortlichen und dem Auftraggeber gelten; eine Zusicherung des Auftraggebers ersetzt sie nicht. Weichen sie von diesem Vertrag ab, teilt er das **vor Beginn der Verarbeitung** in Textform mit; der Auftragsverarbeiter erklärt binnen **14 Tagen**, ob er sie übernimmt. **Andernfalls beginnt die Verarbeitung für diesen Verantwortlichen nicht**; der Auftraggeber kann insoweit außerordentlich kündigen. **Ist der Verantwortliche am Ende der Kette eine öffentliche Stelle, gelten § 1 Abs. 7, § 1 Abs. 8 und § 2 Abs. 5 entsprechend mit der Maßgabe, dass der Auftraggeber die dortigen Mitteilungen für ihn abgibt und die vom Auftragsverarbeiter übernommenen Anforderungen an ihn weitergibt.**

c) **Angaben für das Verzeichnis.** Vor Beginn nennt der Auftraggeber je Verantwortlichem Name und Kontaktdaten, **gegebenenfalls dessen Vertreter nach Art. 27 DSGVO** und **dessen Datenschutzbeauftragten**; ohne sie kann der Auftragsverarbeiter sein Verzeichnis nach Art. 30 Abs. 2 lit. a DSGVO nicht führen.

d) **Verbraucher.** Entwickler-Zugänge sind für Verbraucher (§ 13 BGB) nicht buchbar (AGB § 3 Abs. 8).

(5) **Nur soweit der Auftraggeber Verantwortlicher ist.** Dieser Vertrag regelt eine Auftragsverarbeitung und gilt deshalb nur, soweit der Auftraggeber für die eingebrachten Daten Verantwortlicher ist. Nutzt eine natürliche Person den Arbeitsbereich ausschließlich für persönliche oder familiäre Tätigkeiten (Art. 2 Abs. 2 lit. c DSGVO) und hat sie das dem Auftragsverarbeiter nach Abschnitt 1 seiner Datenschutzerklärung mitgeteilt, ist sie insoweit nicht Verantwortliche; es liegt dann keine Auftragsverarbeitung vor, und der Auftragsverarbeiter ist für diese Inhalte selbst Verantwortlicher. Ohne diese Mitteilung wird vorsorglich Auftragsverarbeitung angenommen. Die Zustimmung zu diesem Vertrag bei der Registrierung begründet für eine rein private Nutzung keine Pflichten, die das Gesetz dem Verantwortlichen auferlegt.

1. Gegenstand der Verarbeitung

Bereitstellung und Betrieb der nach dem Hauptvertrag beauftragten Leistung (Präambel), einschließlich Speicherung, Verarbeitung, Übermittlung und Nutzung der eingegebenen Daten zur Erbringung der vereinbarten Funktionen.

2. Dauer der Verarbeitung

Für die Dauer des Hauptvertrags. Nach dessen Beendigung endet sie gemäß § 7.

3. Art und Zweck der Verarbeitung

Zweck ist ausschließlich die Erbringung der im Hauptvertrag vereinbarten Dienste. Art: Erhebung, Speicherung, Verarbeitung (einschließlich KI-gestützter Analyse, soweit die Suite genutzt wird), Übermittlung, Bereitstellung, Abruf und Löschung über die jeweils genutzte Infrastruktur.

4. Art der personenbezogenen Daten

Je nach genutzten Modulen, soweit das jeweilige Modul für den Verantwortlichen freigeschaltet ist:

- **Stammdaten:** Name, E-Mail-Adresse, Telefonnummer, Anschrift, Organisationszugehörigkeit
- **Kommunikationsinhalte:** Chat-Verläufe, KI-Antworten, Notizen, Aufgaben, Kalendereinträge sowie Inhalte, Anhänge und Teilnehmerkennungen des Messenger-Moduls
- **E-Mail-Daten:** Kopfdaten (Absender, Empfänger, Kopie, Blindkopie, Betreff) und Inhalte ein- und ausgehender Nachrichten samt Anhängen, auch von unbeteiligten Korrespondenzpartnern
- **Verkehrsdaten:** Log-Daten, Nutzungsstatistiken, Zeitstempel, IP-Adressen, Browser- und Gerätekennungen
- **Audio-/Sprachdaten:** Sprachaufnahmen — in der KI-Telefonie transient —, hochgeladene Tondateien Dritter, Transkripte samt Zeitmarken und Sprecherzuordnung, Zusammenfassungen und Analysen von Gesprächen sowie daraus abgeleitete Aufgabenvorschläge, Ruf- und Zielrufnummern und ein anruferbezogenes Gedächtnis (KI-Telefonie)
- **Bild- und Tondaten:** Video- und Audioströme aus Videokonferenzen, auch externer Teilnehmer; eine Aufzeichnungsfunktion **stellt der Auftragsverarbeiter Kunden nicht bereit**
- **Transaktions-, Bank- und Steuerdaten:** Abrechnungsdaten des Verantwortlichen, Bankverbindungen (IBAN), Steuer- und Umsatzsteuer-Identifikationsnummern von Geschäftspartnern, Belegdaten und der per Texterkennung erzeugte Volltext hochgeladener Belege; die Abrechnung des Hauptvertrags samt Credit-Verbrauch ist nicht Gegenstand dieses AVV (Ziff. 0 Abs. 2)
- **Inhaltsdaten:** Dokumente, Dateien, Medien und deren Inhalte, Wissensdatenbanken, Exposé-Daten sowie Standortdaten (Geokoordinaten) im Immobilien-Modul
- **Termin- und Buchungsdaten Dritter:** Name, E-Mail-Adresse, Telefonnummer, Freitextantworten und Absagegründe von Gästen öffentlicher Terminbuchungsseiten

Auf besondere Kategorien (Art. 9 Abs. 1 DSGVO) sind die Dienste nicht ausgerichtet, schließen ihren Anfall aber nicht aus — in freien Text-, Sprach- und Dokumentfeldern und bei Vorlagen des Auftragsverarbeiters (z. B. Terminvereinbarung für Arztpraxis oder Bürgeramt). Über den Einsatz entscheidet der Verantwortliche; er stellt die Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO sicher und teilt eine regelmäßige Verarbeitung solcher Daten vor Beginn in Textform mit. Der Auftragsverarbeiter trifft dann mit ihm die nach Art. 32 DSGVO erforderlichen Zusatzmaßnahmen — Transkriptspeicherung abgeschaltet, Aufbewahrung auf dem Regelwert der Anlage 2, soweit verfügbar Anbieter mit Verarbeitung in der Europäischen Union (§ 4 Abs. 5 und Abs. 6); für die Kanäle, in denen solche Daten ohne Transkript anfallen — Postfächer, Messenger einschließlich der Brücken, Videokonferenzen, Dokumente —, mindestens

die Sperre nach § 4 Abs. 5b oder die Beschränkung nach § 4 Abs. 5a — und unterstützt ihn nach § 6 Abs. 4 bei einer Datenschutz-Folgenabschätzung.

Für öffentliche Stellen mit Bürgertelefon greift ein anderer Satz Maßnahmen, und zwar aus einem Grund, der in der Sache liegt. Am Bürgertelefon eines Sozial-, Ausländer- oder Ordnungsamts nennt ein Anrufer Angaben zu Gesundheit, Herkunft oder Religion nicht ausnahmsweise, sondern regelmäßig und unvermeidbar — er beschreibt sein Anliegen. Die Abschaltung der Transkriptspeicherung nähme der Stelle genau die Funktion, für die sie den Kanal beschafft, und die Anlage 1 ihr für Art. 6 Abs. 1 lit. e gerade eröffnet hat.

Auslöser. Der Verantwortliche teilt dem Auftragsverarbeiter **vor Beginn in Textform** (§ 1 Abs. 2) mit, dass er im Sprachkanal regelmäßig besondere Kategorien verarbeitet, und benennt dabei **gesondert von seiner Rechtsgrundlage nach Art. 6** die Grundlage nach **Art. 9 Abs. 2 lit. b, g oder h DSGVO**. Beides ist zweierlei; die Mitteilung nach Anlage 1 trägt nur die erste. **Welche Grundlage trägt, beurteilt der Verantwortliche**, der Auftragsverarbeiter prüft sie nicht.

Was an die Stelle der Abschaltung tritt — und warum es mehr ist als der Auslieferungszustand. Die nachstehenden Maßnahmen sind **Obergrenzen und Verbote, keine Voreinstellungen**; sie verdrängen für diese Arbeitsbereiche die abweichende Vereinbarung der Anlage 2 und die Wahlmöglichkeit des Arbeitsbereichs:

1. **Die Aufbewahrung ist begrenzt, und zwar für alle drei Bestände, in denen dieselbe Angabe landet** — nicht nur für den Gesprächstext:

Bestand	Obergrenze für diese Arbeitsbereiche	Höchstwert der Anlage 2, der insoweit **nicht** gilt
Gesprächstext (Voice-Transkripte)	**30 Tage**	365 Tage
Call-Metadaten	**90 Tage**	365 Tage
Anruferbezogenes Gedächtnis	**90 Tage ab dem letzten Anruf**	nicht bestimmt

   Eine entgegenstehende Einstellung im Arbeitsbereich ist keine wirksame Weisung nach § 1 Abs. 2, und der Auftragsverarbeiter führt sie nicht aus, sondern teilt sie unverzüglich mit.

   Eine Ausnahme, und nur eine: Trifft den Verantwortlichen für einen dieser Bestände eine **gesetzliche Aufbewahrungspflicht**, die über die Obergrenze hinausgeht — etwa aus dem Archivrecht seines Landes oder der Aktenmäßigkeit des Verwaltungsverfahrens —, so gilt sie vor. **Er benennt sie dem Auftragsverarbeiter in Textform unter Angabe der Vorschrift und der Frist**; ohne diese Benennung bleibt es bei der Obergrenze. **Die Benennung ist keine Einstellung im Arbeitsbereich und wird nicht dort vorgenommen** — sonst wäre die Obergrenze über den Umweg einer behaupteten Pflicht doch abwählbar. Ohne diesen Absatz verböte dieser Vertrag einer Behörde, was ihr eigenes Recht ihr gebietet. Ohne diese Obergrenzen wären die Zahlen die Regelwerte, die jeder Arbeitsbereich ohnehin hat und selbst hochsetzen kann. **Die Beschränkung allein auf den Gesprächstext trüge nicht:** Wer am Bürgertelefon eine Gesundheitsangabe nennt, hinterlässt sie in der Anliegenkategorie der Metadaten und im anruferbezogenen Gedächtnis genauso — und für Letzteres weist Anlage 2 überhaupt keinen Höchstwert aus.
2. **Die automatisierte Gesprächsnachbereitung darf nicht aktiviert werden** — Zusammenfassung, Stimmung, Bewertung erzeugen aus dem Gesagten neue Aussagen über die Person. Auch hier gilt: Eine gleichwohl vorgenommene Aktivierung ist keine wirksame Weisung.

3. **Eingesetzt werden ausschließlich Empfänger des Teils B der Anlage 3**, für die diese Anlage Sitz und Verarbeitung im EWR oder einen Angemessenheitsbeschluss ausweist. Das ist die Beschränkung nach § 4 Abs. 5a, für öffentliche Stellen ohnehin die Voreinstellung — **hier ist sie unabwählbar, und zwar durch keinen der drei Wege, die sie sonst öffnen:**

   - **Eine Weisung, die sie aufhebt, ist insoweit unwirksam** — auch in der Form, in der dieser Vertrag geschlossen wurde. § 4 Abs. 5a gilt für diese Arbeitsbereiche nur in eine Richtung.
   - **Die Abschnitte C und D des Leistungsscheins tragen für den Sprachkanal keine Zeile.** Eine gleichwohl eingetragene Wahl bleibt ohne Wirkung — **auch die eines Empfängers mit Sitz im EWR, für den Anlage 3 eine Weiterübermittlung in ein Drittland ausweist.** Genau dieser Fall ist der praktisch wahrscheinliche: Ein zweiter Telefonieanbieter kann im EWR sitzen und seine Anrufe gleichwohl an eine Gesellschaft in den Vereinigten Staaten weiterreichen.
   - **Der Auftragsverarbeiter darf die Beschränkung nicht „insoweit nicht einrichten".** Liegt die Rufnummer eines Arbeitsbereichs bei einem Anbieter, den Teil B nicht führt, stellt er sie vor der Einrichtung um oder **nimmt den Sprachkanal nicht in Betrieb**; das gilt nach § 4 Abs. 5a und Buchstabe d des Teils B der Anlage 3 ohnehin für jede Beschränkung auf Teil B und ist hier nur benannt, damit der Satz vollständig ist.
4. **Die Unterrichtung zu Gesprächsbeginn nach Anlage 1 bleibt aktiv**; sie ist dort bereits nicht abschaltbar und wird hier nur benannt, damit der Satz vollständig ist.

Was dieser Satz nicht ersetzt. Er gilt für den **Sprachkanal**. Für besondere Kategorien, die außerhalb davon anfallen — in freien Text- und Dokumentfeldern, Notizen, Dateien —, bleibt es beim vorstehenden Absatz einschließlich der abgeschalteten Transkriptspeicherung, soweit sie dort überhaupt Gegenstand ist.

Stützt sich der Verantwortliche auf Art. 9 Abs. 2 lit. h, gilt zusätzlich: Die Verarbeitung ist nur unter den Bedingungen des **Art. 9 Abs. 3 DSGVO** zulässig. Der Verantwortliche teilt das mit der Mitteilung nach **§ 2 Abs. 5** mit; erst daraufhin verpflichtet der Auftragsverarbeiter die befassten Personen auf die dort genannte Geheimhaltungspflicht. **Ohne diese Mitteilung trifft er die Vorkehrung nicht** — und ohne die Vorkehrung trägt lit. h nicht.

Die Unterstützung bei der Datenschutz-Folgenabschätzung nach § 6 Abs. 4 bleibt unberührt; bei einem Bürgertelefon ist sie nach Art. 35 Abs. 3 lit. b DSGVO regelmäßig erforderlich.

5. Kategorien betroffener Personen

- Beschäftigte und Auftragnehmer des Verantwortlichen
- Kunden, Interessenten und Geschäftspartner des Verantwortlichen
- Kontaktpersonen Dritter, soweit vom Verantwortlichen eingegeben
- Anruferinnen und Anrufer der KI-Telefonie und Nutzer des Web-Sprach-/Chat-Widgets, auch ohne Vertragsbeziehung zum Verantwortlichen
- Absender und Empfänger ein- und ausgehender E-Mails
- Gesprächspartner im Messenger-Modul, auch in angebundenen Fremdnetzen. Brücken zu WhatsApp und Telegram sind abgeschaltet und entstehen erst, wenn der Verantwortliche ein eigenes Konto verbindet; diese Aktivierung ist eine dokumentierte Weisung. Für Telegram setzt sie eine für den Vorgang tragfähige Ausnahme nach Art. 49 DSGVO oder einen vom Verantwortlichen sichergestellten Übermittlungsmechanismus voraus; regelmäßige oder massenhafte Übermittlungen dürfen nicht allein auf Art. 49 gestützt werden, und für Verarbeitungen in Ausübung hoheitlicher Befugnisse gilt § 1 Abs. 8
- Gäste öffentlicher Terminbuchungsseiten des Verantwortlichen
- Teilnehmerinnen und Teilnehmer von Videokonferenzen, auch externe Gäste

- Personen, die in eingegebenen Inhalten (Dokumente, Belege, Notizen, Prompts) genannt werden

6. Rechte und Pflichten des Verantwortlichen

Der Verantwortliche bleibt allein verantwortlich für die Rechtmäßigkeit der Verarbeitung. Er ist berechtigt und verpflichtet, Weisungen zu erteilen (§ 1), die Einhaltung dieses AVV zu kontrollieren (§ 8), Betroffenenrechte sicherzustellen und den Auftragsverarbeiter dabei in Anspruch zu nehmen (§ 5) sowie ihn unverzüglich über festgestellte Weisungsverstöße zu informieren.

§ 1 Weisungsgebundenheit (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unions- oder mitgliedstaatlichem Recht zur Verarbeitung verpflichtet; dann teilt er die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht die Mitteilung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

(2) Weisungen erteilt der Verantwortliche in Textform (E-Mail genügt). **Hat er keine weisungsberechtigten Personen benannt, gelten die Inhaber und Administratoren seines Arbeitsbereichs als weisungsberechtigt**; eine Benennung in der Tabelle „Kontaktstellen“ oder später in Textform geht vor. Der Auftragsverarbeiter führt ein **Weisungsregister** mit Datum, Inhalt und ausführender Person jeder Weisung, legt es auf Verlangen vor und bestätigt auf Verlangen in Textform, wen er derzeit als weisungsberechtigt führt. **Einstellungen, die eine weisungsberechtigte Person in der Anwendung selbst vornimmt — insbesondere die Auswahl der KI-Anbieter, die Drittland-Weisung und die Sperre nach § 4 Abs. 5 und 5b und die Aufbewahrungseinstellungen des Arbeitsbereichs —, gelten als dokumentierte Weisung nach Absatz 1; der Auftragsverarbeiter protokolliert sie und weist auf Verlangen nach, welche Person die Einstellung wann vorgenommen hat. Die Anwendung nimmt Drittland-Weisung und Sperre nach § 4 Abs. 5 und 5b in einem Arbeitsbereich eines Unternehmens oder einer öffentlichen Stelle nur von dessen Inhabern und Administratoren an.** Benennt der Verantwortliche weisungsberechtigte Personen, bildet er die Benennung ab, indem er nur ihnen eine dieser Rollen gibt; eine eigene Benennungsliste führt die Anwendung nicht. Erfährt der Auftragsverarbeiter, dass eine Drittland-Weisung von einer nicht benannten Person stammt, führt er sie nicht aus und teilt das dem Verantwortlichen unverzüglich mit.

Wo die Auswahl der Empfänger festgehalten wird. Ist ein Leistungs- und Anbieterschein geschlossen, halten die Parteien dort fest, welcher Empfänger für welche Leistung eingesetzt wird — der Verantwortliche kreuzt je Leistung an, ob der Regelweg oder ein abweichend gewählter Empfänger gilt. **Eine Einstellung, die eine weisungsberechtigte Person in der Anwendung selbst vornimmt, bleibt eine dokumentierte Weisung nach diesem Absatz**; festgehalten wird sie im Protokoll nach Unterabsatz 1 Satz 4. Auf Verlangen bestätigt der Auftragsverarbeiter die in einem Kalendermonat vorgenommenen Einstellungen in Textform, als Auszug aus diesem Protokoll.

(3) Weisungen führt er auch aus, wenn sie über den vereinbarten Leistungsumfang hinausgehen; Mehraufwand teilt er unverzüglich mit und rechnet ihn nach § 5 Abs. 3 ab, ohne die Ausführung von einer Einigung über die Vergütung abhängig zu machen. Ist eine Weisung technisch unmöglich, teilt er das unverzüglich mit Gründen mit und schlägt eine gleichwertige Umsetzung vor.

(4) Hält er eine Weisung für datenschutzrechtlich unzulässig, informiert er den Verantwortlichen unverzüglich; er darf die Ausführung bis zur Klärung aussetzen.

(5) Weisungen umfassen auch die Übermittlung in Drittländer; ohne ausdrückliche Weisung findet keine statt, es sei denn, dieser AVV (Anlage 3) sieht sie vor.

(6) **Behördliche Herausgabeverlangen.** *Aus Drittstaaten:* Verlangt eine Behörde oder ein Gericht außerhalb der EU/des EWR Herausgabe oder Offenlegung von Daten des Verantwortlichen, gibt der Auftragsverarbeiter sie nicht heraus, soweit ihm das rechtlich möglich ist. Sie kommt nur auf Grundlage einer internationalen Übereinkunft im Sinne

von Art. 48 DSGVO oder einer sonst unionsrechtlich zulässigen Grundlage in Betracht, beschränkt auf das zwingend Erforderliche, nach Prüfung von Rechtsmitteln und mit den nach Art. 32 der Verordnung (EU) 2023/2854 gebotenen Maßnahmen gegen rechtswidrigen behördlichen Zugriff. Er unterrichtet den Verantwortlichen unverzüglich, sofern ihm das nicht untersagt ist; ist es untersagt, wirkt er auf die Aufhebung hin und dokumentiert das. Über solche Verlangen führt er ein Verzeichnis und legt es nach § 8 Abs. 1 vor.

Aus dem Inland und der Union: **Für Herausgabe-, Auskunfts- und Beschlagnahmeverlangen deutscher oder in der Union ansässiger Behörden und Gerichte gilt:** Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, soweit ihm das nicht untersagt ist, beschränkt die Herausgabe auf das rechtlich Gebotene, weist die anordnende Stelle auf eine ihm nach § 2 Abs. 5 mitgeteilte Amts- oder Berufsverschwiegenheit und auf die Rechtsstellung des Verantwortlichen hin und nimmt den Vorgang in das Verzeichnis nach diesem Absatz auf. Ist ihm die Unterrichtung untersagt, wirkt er auf die Aufhebung des Verbots hin und dokumentiert das.

(7) **Öffentliche Stellen als Verantwortliche.** Ist der Verantwortliche eine öffentliche Stelle, gelten neben der DSGVO die für ihn maßgeblichen Landesdatenschutzgesetze und bereichsspezifischen Vorschriften. **Dieser Vertrag schließt sie nicht aus und schränkt sie nicht ein**; er verdrängt keine Prüf-, Aufsichts- und Weisungsrechte, die dem Verantwortlichen, seiner Rechtsaufsicht, **seiner örtlichen und überörtlichen Rechnungsprüfung** oder seiner Datenschutzaufsicht danach zustehen. **Zwingendes Recht gilt unabhängig von der folgenden Mitteilung; sie dient allein seiner Umsetzung:** Anforderungen daraus teilt er vor Beginn der Verarbeitung in Textform mit; der Auftragsverarbeiter erklärt binnen **14 Tagen**, ob er sie übernimmt. Andernfalls beginnt die Verarbeitung insoweit nicht, und der Verantwortliche kann diesen AVV außerordentlich kündigen. **Die Landesdatenschutzgesetze legt der Auftragsverarbeiter nicht aus; Rechtsberatung dazu schuldet er nicht.**

Nicht Gegenstand dieses Vertrags sind Verarbeitungen zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, der Strafvollstreckung oder der Abwehr von Gefahren für die öffentliche Sicherheit (Richtlinie (EU) 2016/680 und die sie umsetzenden Vorschriften). Eine Protokollierung, die den Anforderungen dieser Vorschriften genügt, leistet die Anwendung nicht; das Aktivitätsprotokoll der Anlage 2 ist dafür weder bestimmt noch ausgelegt.

(8) **Grenzen des Art. 49 DSGVO bei hoheitlicher Tätigkeit.** Ist der Verantwortliche eine Behörde und verarbeitet er in Ausübung hoheitlicher Befugnisse, sind die Ausnahmen nach **Art. 49 Abs. 1 Unterabs. 1 lit. a, b und c DSGVO nach Art. 49 Abs. 3 DSGVO nicht anwendbar**; dasselbe gilt für Art. 49 Abs. 1 Unterabs. 2 DSGVO. Die gesonderte Erklärung nach § 4 Abs. 5 kann er insoweit nicht wirksam abgeben; eine gleichwohl abgegebene Erklärung trägt die Übermittlung nicht. **Ein Empfänger, für den Anlage 3 keinen Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) ausweist oder für den das Prüfergebnis die Tragfähigkeit der Garantie nicht bestätigt, steht ihm für diese Verarbeitungen nicht zur Verfügung** — in beiden Fällen bleibt keine Grundlage, auf die er sich stützen könnte: Der Auffangweg des Art. 49 Abs. 1 Unterabs. 1 lit. a DSGVO ist ihm nach Art. 49 Abs. 3 DSGVO verschlossen, und eine Garantie, deren Tragfähigkeit die eigene Prüfung nicht bestätigt, trägt die Übermittlung nicht. Darauf unterrichtet der Auftragsverarbeiter vor der ersten Auswahl (§ 4 Abs. 5).

Einer öffentlichen Stelle bietet der Auftragsverarbeiter darüber hinaus keinen Empfänger außerhalb der Europäischen Union oder des EWR an — gleich, ob sie hoheitlich handelt, und gleich, welcher Mechanismus für den Empfänger besteht. **Einzige Ausnahme ist die Proton AG (Schweiz)** für die System- und Betreiberpost und für die Postfächer, die der Verantwortliche über den Auftragsverarbeiter bezieht; für die Schweiz besteht ein Angemessenheitsbeschluss (Art. 45 DSGVO), und Anlage 3 Teil B Buchstabe a benennt den Weg. Die Anwendung weist die übrigen Empfänger für die als öffentliche Stelle gekennzeichneten Arbeitsbereiche ab (§ 3 Abs. 5); eine Drittland-Weisung, eine Weisung je Agent und ein Kreuz in der Anbieterauswahl öffnen sie nicht. **Dasselbe gilt für die Wege, die an einzelnen Funktionen hängen und ein Drittland berühren** — Kurs-Chart, Kartenkacheln und Ortsauflösung über OpenStreetMap, Push-Benachrichtigungen des Messengers, Telegram-Anbindung und die vom Nutzer selbst einzurichtenden Microsoft-Schnittstellen: Für so gekennzeichnete Arbeitsbereiche stellt die Anwendung

sie nicht bereit. **Nicht erfasst sind Ziele, die der Verantwortliche selbst bestimmt**, etwa die Adresse eines Webhooks oder einer HTTP-Anfrage in einem Ablauf; für sie trägt er die Verantwortung.

Was diese Sperre nicht erfasst: Die Ausnahmen des **Art. 49 Abs. 1 Unterabs. 1 lit. d bis g DSGVO** bleiben anwendbar. Will der Verantwortliche eine Übermittlung darauf stützen — insbesondere auf wichtige Gründe des öffentlichen Interesses, die nach **Art. 49 Abs. 4 DSGVO** im Unions- oder mitgliedstaatlichen Recht anerkannt sein müssen —, ist das eine Weisung in der Form, in der dieser Vertrag geschlossen wurde, mit eigener Begründung; sie setzt eine gesonderte Vereinbarung in dieser Form voraus, weil der Auftragsverarbeiter einer öffentlichen Stelle nach dem vorstehenden Unterabsatz keinen Drittland-Empfänger bereitstellt; auf die Rechtsfolgen weist er nach § 1 Abs. 4 hin.

Welche seiner Verarbeitungen in Ausübung hoheitlicher Befugnisse erfolgen, beurteilt der Verantwortliche; **ändert sich seine Beurteilung, teilt er das in Textform mit**, der Auftragsverarbeiter stellt die betroffenen Verarbeitungen mit Zugang der Mitteilung um und bestätigt die Umstellung in Textform.

(9) **Hinweis auf den KI-Charakter bei öffentlichen Stellen.** Für Arbeitsbereiche eines Verantwortlichen, der eine öffentliche Stelle ist, **hält der Auftragsverarbeiter die Ansage zu Gesprächsbeginn aktiv**, mit der auf den KI-Charakter der Kommunikation hingewiesen wird. Er schaltet sie für diese Arbeitsbereiche nicht ab; **eine entgegenstehende Einstellung in der Anwendung ist keine wirksame Weisung nach Absatz 2, und er führt sie nicht aus, sondern teilt sie dem Verantwortlichen unverzüglich mit.** Eine Abweichung setzt eine Weisung in der Form voraus, in der dieser Vertrag geschlossen wurde; auf ihre Rechtsfolgen weist der Auftragsverarbeiter nach Absatz 4 hin.

Die Offenlegungspflicht nach Art. 50 Abs. 1 der Verordnung (EU) 2024/1689 trifft den Auftragsverarbeiter als Anbieter (Ziff. 1.5 der Einsatzbedingungen der KI-Systeme) und bleibt von einer solchen Weisung unberührt. Der Verantwortliche muss sie daher nicht auf anderem Weg erfüllen; im Telefonkanal steht dafür auch keine Oberfläche zur Verfügung, und ein verlinktes Dokument genügt Art. 50 Abs. 5 nicht. **Die Ausnahme für offensichtliche Fälle nach Art. 50 Abs. 1 Satz 1 Halbsatz 2 der Verordnung (EU) 2024/1689 trägt beim Anruf einer Bürgerin oder eines Bürgers bei einer Behörde regelmäßig nicht.**

§ 2 Vertraulichkeit der Verarbeitungsbefugten (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

(1) Alle zur Verarbeitung befugten Personen sind zur Vertraulichkeit verpflichtet — durch schriftliche Verpflichtung oder kraft gesetzlicher Verschwiegenheitspflicht.

(2) **Soweit ausschließlich der Geschäftsführer Zugang zu personenbezogenen Daten hat**, genügt § 85 GmbHG dafür nicht: Er schützt Geheimnisse der Gesellschaft, nicht die Daten des Verantwortlichen, und wird nur auf Antrag verfolgt, den hier niemand stellen kann (§ 85 Abs. 3 GmbHG). **Der Geschäftsführer gibt deshalb eine gesonderte schriftliche Vertraulichkeits- und Weisungsverpflichtung ab**; sie liegt derzeit nicht vor und ist als Maßnahme zum Termin des § 3 Abs. 1 geführt.

(3) Zugang erhalten nur Personen, die ihn zur Erfüllung des Hauptvertrags benötigen (Need-to-know-Prinzip).

(4) **Weisungsbindung der eingesetzten Personen (Art. 29, Art. 32 Abs. 4 DSGVO):** Ihm unterstellte Personen mit Zugang verarbeiten die Daten nur auf Weisung des Verantwortlichen, es sei denn, sie sind unionsrechtlich oder mitgliedstaatlich zur Verarbeitung verpflichtet. Diese Bindung geht in der Vertraulichkeit nach Absatz 1 nicht auf; sie wird mit der Vertraulichkeitserklärung ausdrücklich erklärt und dokumentiert.

(5) **Besondere Geheimhaltungspflichten des Verantwortlichen.** Unterliegt der Verantwortliche für die eingebrachten Daten einer strafbewehrten Berufs- oder Amtsverschwiegenheit oder einem besonderen Geheimnisschutz — insbesondere § 203 StGB, § 35 SGB I, § 30 AO oder einer landesrechtlichen Verschwiegenheitspflicht —, teilt er das **vor Beginn der Verarbeitung** in Textform mit. Der Auftragsverarbeiter verpflichtet die beteiligten Personen dann

zusätzlich nach dieser Vorschrift, beschränkt den Kreis der Zugriffsberechtigten entsprechend und weist beides in Textform nach. **Ohne diese Mitteilung trifft er die Vorkehrungen nicht** — aus den Daten selbst ist nicht erkennbar, welcher Geheimnisschutz gilt. **Sollen Sozialdaten im Sinne des § 67 Abs. 2 SGB X verarbeitet werden, prüft der Verantwortliche vor Beginn die zusätzlichen Voraussetzungen des § 80 SGB X** und teilt dem Auftragsverarbeiter mit, welche Erklärungen, Nachweise oder Genehmigungen er dafür benötigt; der Auftragsverarbeiter stellt sie im Rahmen des § 6 Abs. 1 bereit.

§ 3 Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Der Auftragsverarbeiter **schuldet** die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOM) für ein dem Risiko angemessenes Schutzniveau und trifft sie nach Maßgabe der **Anlage 2**. Dort als offen ausgewiesene Maßnahmen sind noch nicht wirksam; die Pflicht aus Satz 1 bleibt davon unberührt.

Er setzt sämtliche in Anlage 2 als offen geführten Maßnahmen und sämtliche dort unter „Bereiche mit benannten Lücken“ aufgeführten Punkte zu den je Maßnahme im Maßnahmenregister geführten Terminen um, spätestens bis zum 31.12.2026 — einschließlich der Löschlücken (§ 7 Abs. 5), der Verpflichtung des Geschäftsführers (§ 2 Abs. 2) und der Anbieterfestlegungen (§ 4 Abs. 5 und Abs. 6). Die Termine je Maßnahme nennt er unaufgefordert in Textform und weist die Umsetzung ebenso nach.

Wird eine Maßnahme nicht rechtzeitig wirksam, teilt er das unaufgefordert in Textform mit und nennt einen neuen Termin; bleibt sie auch dann aus, kann der Verantwortliche **diesen AVV** außerordentlich kündigen, sofern sie für seine Verarbeitung erheblich ist — das Recht zur Kündigung des Hauptvertrags aus wichtigem Grund bleibt unberührt. Das Risiko der offenen Maßnahmen bewertet er nach Art. 32 Abs. 1 DSGVO, legt die Bewertung offen und wählt die ausgleichenden Maßnahmen; der Verantwortliche entscheidet danach für seine eigene Verarbeitung (Art. 24 Abs. 1 DSGVO). Über den Umsetzungsstand unterrichtet er auf Verlangen, mindestens vierteljährlich in Textform.

(2) Er darf die TOM weiterentwickeln, soweit das Schutzniveau nicht unterschritten wird; über wesentliche Änderungen informiert er vorab in Textform.

(3) Die TOM sind Mindeststandard. Weitergehende Maßnahmen kann der Verantwortliche durch Weisung nach § 1 vorgeben; Mehrkosten trägt er.

(4) **Wiedererlangbarkeit der Daten bei Ausfall des Auftragsverarbeiters.** Der Auftragsverarbeiter hinterlegt den Schlüssel, mit dem verschlüsselt gespeicherte Bestände geschützt sind, **außerhalb der Umgebung, in der diese Bestände liegen**; ohne ihn bleiben sie auch in einer wiederhergestellten Sicherung unlesbar. Die Herausgabe ist an im Voraus bestimmte Bedingungen geknüpft. **Damit kann der Verantwortliche seine Daten auch dann aus einer Sicherung wiedererlangen, wenn der Auftragsverarbeiter ausfällt** (Art. 32 Abs. 1 lit. c DSGVO, § 7). Die Hinterlegung richtet er bis zum Termin des Absatzes 1 ein und weist Art, Stelle und Herausgabebedingungen auf Verlangen in Textform nach; bis dahin weist Anlage 2 den Stand aus, und Absatz 1 gilt mit Mitteilungspflicht und außerordentlichem Kündigungsrecht.

Nicht zugesagt ist der Weiterbetrieb der Plattform durch einen Dritten. Die dafür zusätzlich erforderlichen Geheimnisse sind bewusst nicht Teil der Hinterlegung — je weniger sie enthält, desto geringer der Schaden ihres Verlusts. **Eine Treuhandlösung ist nicht vereinbart.** Von dieser Hinterlegung zu unterscheiden ist die **Vertretung des Geschäftsführers**, an der die Fristen des § 5 Abs. 2 und des § 6 Abs. 2 hängen; sie ist in Anlage 2 als offene Maßnahme geführt.

Wird über das Vermögen des Auftragsverarbeiters ein Insolvenzverfahren beantragt oder eröffnet, unterrichtet er den Verantwortlichen unverzüglich; dieser kann dann Rückgabe und Löschung nach § 7 sofort verlangen und diesen AVV außerordentlich kündigen. § 103 InsO bleibt unberührt.

(5) **Hinweis auf den KI-Charakter bei öffentlichen Stellen — Umsetzungsstand.** Die Zusage steht in **§ 1 Abs. 9**. Solange sie nicht technisch erzwungen wird, ist sie eine organisatorische Maßnahme; sobald sie erzwungen wird, weist Anlage 2 sie als Maßnahme nach Art. 32 DSGVO aus. **Woran der Auftragsverarbeiter einen Arbeitsbereich einer öffentlichen Stelle erkennt, ist die nach Anlage 5 geschlossene Vereinbarung**; nach ihr kennzeichnet er den Arbeitsbereich vor Aufnahme des Betriebs als öffentliche Stelle, und an dieser Kennzeichnung setzt die Anwendung die Ansage technisch durch (Anlage 2). **Von der Voreinstellung nach § 4 Abs. 5a setzt die Anwendung an der Kennzeichnung nur einen Teil technisch durch:** Sie weist jeden Empfänger außerhalb der Europäischen Union ab (§ 1 Abs. 8), und sie versendet für einen so gekennzeichneten Arbeitsbereich keine Kurznachrichten über die Twilio Ireland Limited. Die übrigen Empfänger außerhalb des Teils B — insbesondere Azure OpenAI als Gesprächsmodell und Rufnummern bei der Twilio Ireland Limited — stellt der Auftragsverarbeiter bei der Einrichtung des Arbeitsbereichs um, für die KI-Anbieter über die Anbietersperre des Arbeitsbereichs; insoweit ist die Voreinstellung eine organisatorische Maßnahme.

(6) **Dedizierte Instanz für öffentliche Stellen.** Personenbezogene Echtdaten einer öffentlichen Stelle verarbeitet der Auftragsverarbeiter **ausschließlich auf einer dedizierten Instanz**, die der öffentlichen Stelle zugeordnet ist und nicht mit Arbeitsbereichen anderer Verantwortlicher geteilt wird. Für diese Instanz gilt: (a) **eigener Server in Deutschland**; (b) **vollständige Datenträgerverschlüsselung**; (c) **verschlüsselte Sicherung außer Haus** — außerhalb des Servers, auf dem die Instanz läuft — **mit regelmäßigem Wiederherstellungstest**, dessen Ergebnis er der öffentlichen Stelle auf Verlangen in Textform vorlegt. **Der Auftragsverarbeiter stellt die Instanz bereit und weist die Merkmale (a) bis (c) der öffentlichen Stelle in Textform nach, bevor diese Echtdaten verarbeiten lässt.** Bis zu diesem Nachweis verarbeitet er für die öffentliche Stelle keine personenbezogenen Echtdaten; Erprobung ist nur mit erfundenen Daten zulässig. Wie die gemeinsame Plattform heute ausgestattet ist, weist Anlage 2 aus. Die Zusage ersetzt die Beschränkungen der Absätze 1 bis 5 und des § 4 nicht, sondern tritt zu ihnen hinzu.

§ 4 Sub-Auftragsverarbeiter (Art. 28 Abs. 2 und Abs. 4 DSGVO)

(1) **Allgemeine Genehmigung:** Der Verantwortliche genehmigt allgemein die Beauftragung der in **Anlage 3** mit der Rolle *AV*, *AV · ohne Art.-28-Vertrag* oder *beides* geführten Sub-Auftragsverarbeiter. Für die übrigen Empfänger ist der Auftragsverarbeiter selbst Verantwortlicher (Ziff. 0 Abs. 2) oder es besteht kein Auftragsverhältnis; die mit *selbst* gekennzeichneten Dienste auf eigener Infrastruktur verarbeiten im Auftrag, sind aber keine eigenständigen Sub-Auftragsverarbeiter — Absätze 2 und 3 gelten für sie nicht.

Auf Empfänger im Status ***eingerichtet, ruht*, *eingerichtet, nicht in Betrieb* oder *ausgesetzt*** erstreckt sie sich erst mit der Mitteilung nach Absatz 2; **eine Auswahl oder Weisung ersetzt sie nicht (Absatz 2a)**. **Auf Empfänger, die Anlage 3 in der Spalte „Zweck“ mit *Kette nicht abschließend dokumentierbar* ausweist**, erstreckt sie sich mit der Maßgabe des Absatzes 4; auf die dort benannte Lücke wird der Verantwortliche vor der ersten Auswahl hingewiesen.

Eingesetzt wird ein Empfänger erst, wenn Anlage 3 ihn mit Rechtsträger, Sitz, Rolle, Status und Mechanismus führt. Verarbeitet einer gleichwohl im Auftrag, ohne dort mit eigener Zeile und der Rolle *AV* oder *beides* zu stehen, teilt der Auftragsverarbeiter das unverzüglich mit, holt die Mitteilung nach Absatz 2 nach und setzt ihn bis dahin nicht ein.

(2) **Informationspflicht vor Änderungen:** Über beabsichtigte Änderungen — Hinzufügung oder Ersetzung von Sub-Auftragsverarbeitern sowie die erstmalige Inbetriebnahme eines nach Absatz 1 im Status *eingerichtet, ruht*, *eingerichtet, nicht in Betrieb* oder *ausgesetzt* geführten Empfängers — informiert der Auftragsverarbeiter mindestens **30 Tage** vor dem geplanten Einsatz in Textform. **Die Information ergeht per E-Mail an die im Abschluss benannte Kontaktstelle des Verantwortlichen, hilfsweise an die E-Mail-Adresse des Inhabers des Arbeitsbereichs; maßgeblich für den Beginn der Frist ist der Zugang der E-Mail. Zeitgleich führt der Auftragsverarbeiter Anlage 3 nach, die unter /trust/subprozessoren öffentlich abrufbar ist.** <!-- R5-CODE: Der Versand ist ein manueller Prozess des Betreibers (Register Nr. 260), solange das Produkt keinen Verteiler hat. -->

(2a) **Keine Inbetriebnahme durch bloße Auswahl oder automatischen Rückfall.** Jeder neue, ergänzte oder ersetzte Sub-Auftragsverarbeiter muss vor dem ersten Einsatz nach Absatz 2 mitgeteilt und von der allgemeinen Genehmigung erfasst sein — auch innerhalb einer technischen Fallback- oder Aggregatorkette. **Eine Auswahl oder Weisung des Verantwortlichen verkürzt die Mitteilungsfrist nicht.**

(3) **Einspruchsrecht:** Gegen einen neuen oder geänderten Sub-Auftragsverarbeiter kann der Verantwortliche aus berechtigtem Grund in Textform Einspruch erheben, binnen **14 Tagen ab Zugang** der Mitteilung nach Abs. 2. Vor Ablauf der Mitteilungs- und Einspruchsfrist findet kein Einsatz statt.

(3a) **Folgen des Einspruchs:** Die Parteien erörtern unverzüglich eine gleichwertige Alternative; besteht eine, wird der Sub-Auftragsverarbeiter für die Daten des Verantwortlichen nicht eingesetzt. Besteht keine — insbesondere, wenn der Empfänger die Infrastruktur trägt, auf der die Dienste erbracht werden —, teilt der Auftragsverarbeiter das binnen 14 Tagen in Textform mit; der Verantwortliche kann dann diesen AVV und den Hauptvertrag außerordentlich kündigen, und bereits gezahlte Vergütung wird für die Zeit nach Wirksamwerden der Kündigung anteilig erstattet.

(3b) **Zustimmungsvorbehalt statt Widerspruchslösung.** Der Verantwortliche kann in Textform verlangen, dass die Beauftragung neuer oder geänderter Sub-Auftragsverarbeiter **seiner vorherigen Zustimmung** bedarf (Art. 28 Abs. 2 Satz 1 DSGVO). Ab Zugang der Erklärung setzt der Auftragsverarbeiter einen nach Absatz 2 mitgeteilten Empfänger für dessen Daten **erst nach Zustimmung** ein; Schweigen genügt nicht, bei Verweigerung gilt Absatz 3a entsprechend. **Die nach Absatz 1 erteilte allgemeine Genehmigung bleibt für die bei Zugang der Erklärung in Anlage 3 geführten Empfänger bestehen** — sonst stünde die Leistung mit der Erklärung still. Der Vorbehalt ist jederzeit in Textform widerruflich.

(4) **Back-to-Back:** Der Auftragsverarbeiter legt jedem Sub-Auftragsverarbeiter und jedem Unteranbieter vertraglich dieselben Datenschutzpflichten auf, die ihm nach diesem AVV obliegen (Art. 28 Abs. 4 DSGVO), und haftet für deren Pflichtverletzungen nach Art. 28 Abs. 4 Satz 2 DSGVO in vollem Umfang. **Wie sich diese Haftung zur betragsmäßigen Begrenzung des § 9 Abs. 2 verhält, ist dort gesondert bezeichnet und zwischen den Parteien noch nicht festgelegt. Bei einem Aggregator lässt sich der Kreis der Unteranbieter nicht abschließend benennen; für ihn sichert der Auftragsverarbeiter deshalb weder die vollständige Weitergabe der Art.-28-Pflichten noch eine lückenlose Kette nach Kapitel V DSGVO zu, und Anlage 3 weist das aus. Weist Anlage 3 für ihn einen Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) aus, kann der Verantwortliche ihn gleichwohl wählen — die Auswahl ist seine dokumentierte Weisung nach § 1 Abs. 1, und er trägt sie mit den Folgen des Absatzes 5; einen Aggregator ohne solchen Mechanismus bietet der Auftragsverarbeiter nicht an (Absatz 5).**

Wo diese Pflicht nicht erfüllt ist, wird sie ausgewiesen und nicht umgeschrieben. Für einen Empfänger, der im Auftrag verarbeitet, ohne dass ein auf ihn lautender Vertrag nach Art. 28 DSGVO vorliegt, führt Anlage 3 die Rolle ***AV · ohne Art.-28-Vertrag***; der Auftragsverarbeiter unterrichtet darüber vor der ersten Auswahl (Absatz 5) und schuldet den Vertragsschluss unverändert (§ 10 Abs. 1). **Die Rolle ist eine Beschreibung des Ist-Zustands, keine Genehmigung und keine Einschränkung der geschuldeten Pflicht.**

(5) **Drittlandtransfers durch Sub-Auftragsverarbeiter. Grundsatz: Das Ergebnis der Transfer-Folgenabschätzung wird ausgewiesen und nicht als Sperre verwendet — kein Prüfergebnis entzieht dem Verantwortlichen die Wahl unter den Anbietern des Katalogs.** In den Katalog kommt ein Empfänger nur, wenn Anlage 3 ihn konkret bestimmt und Rolle, Verarbeitungsort, Mechanismus nach Kapitel V DSGVO und Prüfergebnis ausweist — **einschließlich der Feststellung, dass ein Mechanismus, ein Vertrag nach Art. 28 DSGVO oder eine lückenlose Kette fehlt. Weist Anlage 3 für ihn das Prüfergebnis *trägt nicht* oder eine dieser Lücken aus, unterrichtet der Auftragsverarbeiter vor der ersten Auswahl über Sitz, Verarbeitungsort und Prüfergebnis.** Die Katalogentscheidung als solche darf er technisch durchsetzen.

Vor der ersten Übermittlung in ein Drittland verlangt die Anwendung eine Drittland-Weisung. In einem Arbeitsbereich eines Unternehmens oder einer öffentlichen Stelle erteilen sie **nur dessen Inhaber und**

Administratoren; die Anwendung nimmt sie von anderen Mitgliedern nicht an. Im persönlichen Arbeitsbereich erteilt die Person sie für ihre eigenen Daten selbst. Die Drittland-Weisung ist eine **dokumentierte Weisung nach Art. 28 Abs. 3 Satz 2 lit. a DSGVO und keine Einwilligung** nach Art. 6 Abs. 1 lit. a oder Art. 49 Abs. 1 Unterabs. 1 lit. a DSGVO; die Anwendung protokolliert Person, Zeitpunkt und die Fassung des Hinweistexts, dem sie erteilt wurde (§ 1 Abs. 2). Sie gilt je Arbeitsbereich, **unbefristet und jederzeit widerruflich**; ohne sie spricht der Auftragsverarbeiter keinen Drittland-Empfänger an. **Empfänger, für die Anlage 3 keinen Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) ausweist, werden über die Drittland-Weisung nicht angeboten** — für sie gibt es keine Grundlage, die eine Weisung ersetzen könnte; das betrifft auch die Unteranbieter eines Aggregators, für die Anlage 3 keinen solchen Mechanismus ausweist. **Das gilt auch im persönlichen Arbeitsbereich. Die Anwendung lässt einen solchen Empfänger allerdings nach einer gesonderten Freischaltung je Weg zu**, die Inhaber und Administratoren nach einem Hinweis auf die fehlende Grundlage erteilen; sie öffnet ihn nie für die Daten der Personen nach dem folgenden Satz und nie für Arbeitsbereiche öffentlicher Stellen (§ 1 Abs. 8). **Eine Grundlage nach Kapitel V DSGVO schafft die Freischaltung nicht**, und der erste Einsatz eines in Anlage 3 als ruhend geführten Empfängers bleibt an die Mitteilung nach Absatz 2 gebunden (Absatz 2a); was im Einzelnen gilt, steht in Anlage 3, Festlegung (c). **Für personenbezogene Daten von Personen, die den Empfänger nicht wählen — insbesondere Anruferinnen und Anrufer, Gesprächspartner und Nutzer der Widgets (Ziff. 5 der Präambel) —, genügt die Drittland-Weisung des Arbeitsbereichs nicht.** Ein Agent spricht für sie einen Drittland-Empfänger nur an, wenn ein Inhaber oder Administrator das **für diesen Agenten und diesen Empfänger gesondert und ausdrücklich angewiesen** hat, in Kenntnis des Prüfergebnisses, das Anlage 3 ausweist — für jeden Steckplatz einschließlich der Rückfallebene; die Anwendung protokolliert Person, Zeitpunkt und Fassung des Hinweistexts. **Fehlt diese Weisung, läuft der Agent nicht**; er weicht nicht auf einen anderen Anbieter aus. Empfänger ohne Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) bleiben auch hier ausgeschlossen. Die Rechtsgrundlage gegenüber diesen Personen und ihre Unterrichtung über die Übermittlung stellt der Verantwortliche sicher (§ 9 Abs. 4 lit. a). **Bis zur Fassung 2.42 sagte dieser Absatz zu, ihre Daten gingen an einen Empfänger, dessen Prüfergebnis die Tragfähigkeit nicht bestätigt, auch auf Weisung nicht; an ihre Stelle ist mit Fassung 2.43 die gesonderte Weisung je Agent getreten.** Gegenüber einem Verantwortlichen, der der Fassung 2.43 oder einer späteren noch nicht zugestimmt hat (§ 10 Abs. 2; beim Abschluss über die Anwendung § 9 Abs. 3 der AGB), gilt die frühere Zusage bis zu seiner Zustimmung fort; eine Weisung je Agent wirkt für ihn erst ab diesem Zeitpunkt. Für Verarbeitungen in Ausübung hoheitlicher Befugnisse gilt zusätzlich § 1 Abs. 8.

Wählt der Verantwortliche einen Empfänger, führt der Auftragsverarbeiter die Weisung aus; **die Verantwortung für die Auswahl unter den angebotenen Empfängern trägt der Verantwortliche, die Pflichten aus §§ 1 bis 8 und die Haftung nach § 9 bleiben unberührt. Die Weisung ersetzt weder die Garantie noch eine erforderliche Einwilligung der betroffenen Person** — insbesondere nicht gegenüber Anrufern und Gesprächspartnern, die ihren Anbieter nicht wählen; deren Rechtsgrundlage stellt der Verantwortliche sicher. **Managed betrieben ist jeder Agent, den der Auftragsverarbeiter für den Verantwortlichen einrichtet oder pflegt, und jeder Agent in einem Arbeitsbereich des Verantwortlichen, in dem der Auftragsverarbeiter Inhaber oder Administrator ist.** Vom Auftragsverarbeiter selbst betrieben sind in diesem Vertrag die Agenten der EU-Betriebsarten Sentinel und Cortex; ein Agent, den er allein für eigene Zwecke nutzt, verarbeitet keine Daten des Verantwortlichen und fällt nicht unter diesen Vertrag (Ziff. 0 Abs. 2). Für die managed betriebenen Agenten und für die von ihm selbst betriebenen Agenten der EU-Betriebsarten Sentinel und Cortex setzt der Auftragsverarbeiter — für jeden Steckplatz einschließlich der Rückfallebene — **ausschließlich Empfänger in der Europäischen Union oder dem EWR ein, es sei denn, der Verantwortliche hat einen Drittland-Empfänger in der Anbieterauswahl durch Unterschrift ausgewählt. Eine Drittland-Weisung oder eine Weisung je Agent für einen Drittland-Empfänger erteilt der Auftragsverarbeiter in solchen Arbeitsbereichen nie selbst.** Die unterschriebene Anbieterauswahl ist für die dort angekreuzten Drittland-Empfänger zugleich die gesonderte Weisung je Agent nach dem vorstehenden Unterabsatz, für alle managed betriebenen Agenten, soweit sie sie nicht auf einzelne beschränkt; der Auftragsverarbeiter bildet sie in der Anwendung ab und protokolliert dabei die Nummer der Anbieterauswahl. Das Abbilden ist keine eigene

Weisung. Aggregatoren setzt er dort nicht ein. Ein automatischer Rückfall auf einen nicht gewählten Empfänger ist ausgeschlossen; **ein Rückfall auf denselben Drittlandempfänger vermeidet die Übermittlung nicht, sondern verdoppelt sie.**

(5a) **Beschränkung auf Teil B der Anlage 3.** Der Verantwortliche kann in Textform anweisen, dass für seine sämtlichen Arbeitsbereiche ausschließlich die in **Teil B der Anlage 3** geführten Empfänger eingesetzt werden. **Nicht erfasst sind die Wege, die der Auftragsverarbeiter selbst bestimmt** — Teil B benennt sie unter den Buchstaben a) bis d) abschließend mit Rechtsträger, Sitz und Grundlage, und sie lassen sich durch diese Beschränkung nicht abwählen. **Der Sprachkanal bleibt damit nutzbar**; das ist der Unterschied zur Konfiguration nach Absatz 6a, die ihn ausschließt. **„Teil B“ meint in diesem Absatz die dortige Tabelle zusammen mit den Buchstaben a) bis d)**; wo dieser Vertrag in Absatz 6a von den *Merkmalen* des Teils B spricht, sind die drei kumulativen Merkmale der Tabelle gemeint. **Diese Weisung geht einer in der Anwendung erteilten Drittland-Weisung nach Absatz 5 vor**; eine entgegenstehende Einstellung ist keine wirksame Weisung nach § 1 Abs. 2, und der Auftragsverarbeiter führt sie nicht aus, sondern teilt sie dem Verantwortlichen unverzüglich mit. **Für öffentliche Stellen ist diese Beschränkung die Voreinstellung**; ihre Aufhebung setzt eine Weisung in der Form voraus, in der dieser Vertrag geschlossen wurde.

Der Auftragsverarbeiter **verpflichtet sich**, dass für die Arbeitsbereiche des Verantwortlichen keine Übermittlung an Empfänger außerhalb von Teil B stattfindet; Rufnummern stellt er dafür ausschließlich über die Vonage B.V. bereit, und Kurznachrichten über die Twilio Ireland Limited versendet er für diese Arbeitsbereiche nicht (Teil B Buchstabe d). **Technisch gesperrt ist dieser Versand nur für Arbeitsbereiche, die als öffentliche Stelle gekennzeichnet sind;** für eine Beschränkung, die ein anderer Verantwortlicher verlangt, gibt es in der Anwendung kein eigenes Merkmal — dort stellt der Auftragsverarbeiter den Versand bei der Einrichtung der Beschränkung organisatorisch ab. Er **teilt jede Abweichung unverzüglich und unaufgefordert in Textform mit** und **weist auf Verlangen nach**, welche Empfänger im angefragten Zeitraum für die Arbeitsbereiche des Verantwortlichen angesprochen wurden. § 3 Abs. 5 Satz 2 gilt für diese Beschränkung entsprechend. **Hebt der Verantwortliche die Beschränkung auf, weist der Auftragsverarbeiter darauf hin, dass das eine Überprüfung seiner Datenschutz-Folgenabschätzung nach Art. 35 Abs. 11 DSGVO auslösen kann**; die Zuarbeit richtet sich nach § 6 Abs. 4.

(5b) **Sperre durch den Verantwortlichen.** Inhaber und Administratoren können Drittland-Empfänger für ihren Arbeitsbereich in der Anwendung **sperren**. Die Sperre wird serverseitig bei jedem Aufruf eines KI-Anbieters geprüft, der Inhalte des Arbeitsbereichs übermittelt — aus Chat, Workflows, Agenten, Sprachpfad und Programmierschnittstelle gleichermaßen; kann die Einstellung nicht gelesen werden, gilt sie als gesetzt — und **geht einer erteilten Drittland-Weisung vor**: Solange sie gesetzt ist, spricht der Auftragsverarbeiter für diesen Arbeitsbereich keinen Drittland-Empfänger an, gleich wer die Weisung erteilt hat. Daneben können sie jeden einzelnen Anbieter des Katalogs für ihren Arbeitsbereich abschalten lassen, auch einen mit Verarbeitung in der Europäischen Union; auch diese Abschaltung wird serverseitig bei jedem Aufruf geprüft. **Selbst schalten sie in der Anwendung jeden Anbieter einzeln ab** — Sprachmodelle (je Ressource, bei Azure OpenAI also jede Region einzeln), Spracherkennung, Sprachsynthese, Bilderzeugung und Web-Suche — **und ganze Anbieterfamilien**, etwa Microsoft Azure insgesamt; die Abschaltung gilt auch für Neueinträge der Familie und für die Live-Sprachpfade. **Entfällt dadurch der einzige Anbieter einer Leistung und ist kein vereinbarter Rückfall hinterlegt, endet die Leistung mit einem Hinweis:** So endet der Telefon-Agent ohne Azure mit einer Ansage, solange für die Echtzeit-Spracherkennung kein Rückfall vereinbart ist (Anlage 3 Teil B Buchstabe b). Eine Beschränkung nach Absatz 5a wirkt daneben für sämtliche Arbeitsbereiche des Verantwortlichen.

(6) **Anbieterfestlegungen.**

a) **Spracherkennung.** Azure AI Speech, Region Germany West Central, ist Voreinstellung und für die vom Auftragsverarbeiter selbst sowie managed betriebenen Agenten verbindlich, soweit der Verantwortliche in der Anbieterauswahl nichts anderes gewählt hat; Deepgram ist dort weder Standard noch Fallback. Für eigene Agenten des Verantwortlichen entscheidet dieser.

b) **Sprachsynthese.** Voreinstellung ist **KugelAudio** in der Variante **„EU-Only Hosting“** nach § 13 Abs. 2 der Anbieterbedingungen, auch für die vom Auftragsverarbeiter selbst und die managed betriebenen Agenten, soweit der Verantwortliche in der Anbieterauswahl nichts anderes gewählt hat. **Die Verarbeitung in der Europäischen Union hat der Anbieter am 2026-09-23 bestätigt**; der Auftragsverarbeiter weist sie auf Verlangen nach. Ein automatischer Fallback auf andere Regionen **wird nicht eingerichtet**. **Azure AI Speech**, Region Germany West Central, steht als Alternative mit Verarbeitung in der Europäischen Union zur Wahl. **Solange ein auf die KugelAudio GmbH lautender Vertrag nach Art. 28 DSGVO und die vollständige Subprozessorenkette in Anlage 3 nicht ausgewiesen sind, ist die Verarbeitung insoweit nicht freigegeben** — eine Anforderung an das Soll, keine technische Sperre: **Eingesetzt wird die KugelAudio GmbH gleichwohl** (Anlage 3, Status *in Betrieb*); der Verantwortliche kann in der Anbieterauswahl Azure AI Speech wählen. Vertrag und Kette schuldet der Auftragsverarbeiter nach Absatz 4, erteilt ist allein die Bestätigung des EU-Hostings.

c) **Inhaltssperre der Sprachsynthese-Kette.** Der Anbieter der Sprachsynthese darf Audio-, Text- oder Sprachproben nicht an seine Unterauftragnehmer weitergeben; erhält ein Unteranbieter gleichwohl solche Inhalte, ist er vor dem weiteren Einsatz mit Rechtsträger, Sitz, Rolle und Mechanismus in Anlage 3 auszuweisen. Voice Cloning bleibt separat gesperrt.

d) **Drittlandprovider bleiben katalogsichtbar und wählbar.** Ihre Auswahl ist eine dokumentierte Weisung nach § 1 Abs. 1, auf deren Rechtsfolgen der Auftragsverarbeiter nach § 1 Abs. 4 hinweist; das Verfahren regelt Absatz 5.

e) **Übermittlung nach Rollen getrennt. Wählt der Auftragsverarbeiter den Empfänger** — für die von ihm selbst und die managed betriebenen Agenten sowie für die eigene Infrastruktur —, übermittelt er nur an Empfänger mit Sitz und Verarbeitung in der Europäischen Union oder dem EWR oder an solche, für die Anlage 3 einen Mechanismus nach Art. 45, 46 oder 47 DSGVO **und kein die Tragfähigkeit verneinendes Prüfergebnis** ausweist, und mit denen, soweit sie in seinem Auftrag verarbeiten, ein Vertrag nach Art. 28 Abs. 3 DSGVO besteht. **Wählt der Verantwortliche** — in der Anwendung oder bei managed betriebenen Agenten in der Anbieterauswahl —, gilt Absatz 5; einen Empfänger ohne ausgewiesenen Mechanismus bietet der Auftragsverarbeiter nicht an (Absatz 5).

f) **Aggregatoren.** Vom Aggregator verlangt der Auftragsverarbeiter die vollständige Weitergabe der Art.-28-Pflichten an dessen Unteranbieter und weist den benannten Unteranbieterkreis in Anlage 3 aus. **Überwachen kann er die Einhaltung nicht und sichert sie nicht zu** (Absatz 4); für eigene Assistenten setzt er Aggregatoren nicht ein.

g) **Beispielbilder der Widget-Einstellungen** liefert der Auftragsverarbeiter aus eigener Infrastruktur; ein externer Abruf bei Dritten **ist nicht vorgesehen**.

Den Umsetzungsstand weist Anlage 3 aus; eine dort ausgewiesene Abweichung ist keine Ausnahme von diesen Festlegungen. **Eine Auswahl oder Weisung des Verantwortlichen hebt die Anforderungen der Buchstaben a, b, c, f und g nicht auf.**

(6a) **Konfiguration „Verarbeitung im EWR“.** Auf Verlangen des Verantwortlichen in Textform (Absatz 5a) richtet der Auftragsverarbeiter dessen Arbeitsbereiche so ein, dass **keine Übermittlung an einen Empfänger außerhalb des EWR** stattfindet, für die dieser Vertrag eine Wahl vorsieht: Die Drittland-Weisung nach Absatz 5 wird nicht erteilt, und eine gleichwohl erteilte bleibt nach Absatz 5a ohne Wirkung. **Nicht erfasst sind die Wege, die der Auftragsverarbeiter selbst bestimmt; Teil B der Anlage 3 benennt sie abschließend mit Rechtsträger, Sitz und Grundlage.** Für sie gelten Absatz 6 und die dortigen Vorbehalte unverändert. Die eingerichtete Konfiguration bestätigt der Auftragsverarbeiter in Textform.

Für die **Echtzeit-Spracherkennung** steht kein Anbieter zur Verfügung, der zugleich im EWR ansässig und keiner Verfügungsgewalt eines Drittstaatskonzerns unterworfen ist; kein Anbieter erfüllt damit alle Merkmale des Teils B. **Wählt der Verantwortliche diese Konfiguration, ist der Sprachkanal — KI-Telefonie und Web-Sprach-Widget — insoweit nicht nutzbar.** Wer diese Konfiguration wählt, kreuzt in **Anlage 5** Ziffer 2 Buchstabe b an und den Sprachkanal nicht; die schriftlichen Kanäle bleiben uneingeschränkt nutzbar. **Wie sich die beiden Festlegungen der Ziffer 2**

zueinander verhalten, steht dort — an der Stelle, an der der Verantwortliche wählt. Wird der Sprachkanal später hinzugewählt, **endet die Konfiguration nach diesem Absatz mit seiner Inbetriebnahme**; der Auftragsverarbeiter teilt das dem Verantwortlichen in Textform mit, bevor der Kanal in Betrieb geht.

§ 5 Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 Satz 2 lit. e DSGVO)

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei seinen Pflichten gegenüber betroffenen Personen:

- Auskunft und Datenübertragbarkeit (Art. 15, 20 DSGVO): strukturierte Exporte in Format, Umfang und auf dem Weg des § 7 Abs. 3, innerhalb der Frist des Absatzes 3 und mit Nachweis nach § 7 Abs. 7. **Gegenstand ist der Bestand der betroffenen Person, nicht der des Arbeitsbereichs**; dessen Rückgabe schuldet der Auftragsverarbeiter nach § 7 Abs. 3 dem Verantwortlichen und darf die Selbstbedienungsfunktion dafür an die Eigentümerin oder die Verwaltung des Arbeitsbereichs binden. Gesetzliche Ansprüche bleiben unberührt
- Berichtigung und Löschung (Art. 16, 17 DSGVO): über die Funktionen der Anwendung, ergänzend auf Weisung; die Löschung auf Verlangen einschließlich der endgültigen Entfernung aus Datenbank und Objektspeicher nach § 7 Abs. 5
- Einschränkung und Widerspruch (Art. 18, 21 DSGVO): Umsetzung auf Weisung. Fehlt eine Kennzeichnung als „in der Verarbeitung eingeschränkt“, wird der Datensatz aus dem produktiven Zugriff genommen, unverändert aufbewahrt und die Sperrung dokumentiert; die Aufhebung teilt der Auftragsverarbeiter vorab mit (Art. 18 Abs. 3 DSGVO). Fehlt eine Markierungsfunktion, erfolgt die Umsetzung organisatorisch und unverzüglich nach Zugang der Weisung

(2) Anfragen betroffener Personen leitet der Auftragsverarbeiter unverzüglich, spätestens binnen **72 Stunden** ab Eingang bei ihm, an den Verantwortlichen weiter — die kurze Frist wahrt dessen Monatsfrist nach Art. 12 Abs. 3 DSGVO. Für ein Fristhindernis gilt Absatz 3 Satz 2. Im eigenen Namen beantwortet er sie nur auf ausdrückliche Weisung.

(3) Die Leistungen nach Absatz 1 erbringt er so rechtzeitig, dass der Verantwortliche seine Frist nach Art. 12 Abs. 3 DSGVO wahren kann, spätestens binnen **zehn Arbeitstagen** nach Zugang der Anfrage und unabhängig von einer Einigung über die Vergütung; ein Zurückbehaltungs- oder Leistungsverweigerungsrecht besteht insoweit nicht. Ist eine Frist aus einem von ihm nicht zu vertretenden Grund nicht einzuhalten, leistet er unverzüglich nach Wegfall des Hindernisses und teilt den Grund mit. Enthalten sind die Leistungen, soweit ihr Aufwand **vier Stunden je Vertragsjahr** nicht übersteigt; dieses Freikontingent gilt für § 5 Abs. 1 und § 6 Abs. 3 bis 5 zusammen. Die Bereitstellung nach § 7 Abs. 3 ist davon nicht erfasst; **sie erfolgt entgeltfrei**. Für Mehraufwand kann er eine angemessene Vergütung nach dem vereinbarten Stundensatz verlangen, sonst nach der üblichen Vergütung (§ 632 Abs. 2 BGB), je Vertragsjahr begrenzt auf **10 % der für dieses Vertragsjahr vereinbarten Vergütung des Hauptvertrags**.

(4) **Angaben für die Information der betroffenen Personen (Art. 13, 14 DSGVO).** Die Information der betroffenen Personen obliegt dem Verantwortlichen. Der Auftragsverarbeiter stellt ihm dafür **bei Vertragsbeginn und bei jeder Änderung der Angaben unaufgefordert** in Textform eine **auf seine Arbeitsbereiche bezogene** Zusammenstellung bereit, die mindestens ausweist:

- die **Empfänger oder Kategorien von Empfängern**, die Daten dieser Arbeitsbereiche tatsächlich erhalten;
- ob dabei in ein **Drittland** übermittelt wird und auf welcher **Grundlage nach Kapitel V DSGVO**;

- die für diese Arbeitsbereiche **gesetzten Aufbewahrungsfristen** (Anlage 2), auch soweit sie von den dortigen Regelwerten abweichen.

  Der Empfängerkreis der gesamten Suite genügt dieser Pflicht nicht: Anlage 3 führt alle Empfänger aller Anwendungen; wer sie unverändert übernimmt, nennt den betroffenen Personen Empfänger, die ihre Daten nie erhalten (Art. 5 Abs. 1 lit. a DSGVO). Die Zusammenstellung ist **entgeltfrei**; das Freikontingent des Absatzes 3 gilt für sie nicht.

§ 6 Unterstützung bei Sicherheit und behördlichen Pflichten (Art. 28 Abs. 3 Satz 2 lit. f DSGVO)

(1) **Sicherheit (Art. 32 DSGVO):** Unterstützung bei den Pflichten des Verantwortlichen, insbesondere durch Bereitstellung der in Anlage 2 dokumentierten TOM-Nachweise.

(2) **Meldepflicht Datenpanne (Art. 33 DSGVO):** Der Auftragsverarbeiter meldet jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden, **in der Regel innerhalb von 24 Stunden** — die verkürzte Frist soll dem Verantwortlichen die Zeit für seine eigene 72-Stunden-Meldung (Art. 33 Abs. 1 DSGVO) belassen. Für ein Fristhindernis gilt § 5 Abs. 3 Satz 2; der Vorbehalt entfällt mit der in Anlage 2 als offen ausgewiesenen Vertretungsregelung. **Die Meldung geht per E-Mail an die in den Kontaktstellen benannte Meldestelle** — dieser Weg trägt sie allein, weil er einen nachweisbaren Zeitstempel hinterlässt; ist keine Meldestelle benannt, an die zuletzt bekannte E-Mail-Adresse des Ansprechpartners. Hat der Verantwortliche in den Kontaktstellen eine Rufnummer benannt, ruft der Auftragsverarbeiter zusätzlich dort an; die Frist wahrt jedoch die E-Mail. Sie enthält mindestens Art der Verletzung, Kategorien und ungefähre Anzahl betroffener Personen und Datensätze, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Maßnahmen (Art. 33 Abs. 3 DSGVO). Liegen noch nicht alle Angaben vor, meldet er fristgerecht vorläufig und ergänzt unverzüglich, ohne die Erstmeldung hinauszuzögern.

(3) **Benachrichtigung Betroffener (Art. 34 DSGVO):** Unterstützung auf Weisung.

(4) **Datenschutz-Folgenabschätzung (Art. 35 DSGVO):** Auf Anfrage stellt er alle für eine DSFA erforderlichen Informationen nach Art. 35 Abs. 7 lit. a bis d DSGVO bereit, soweit sie seiner Sphäre entstammen.

(5) **Aufsichtsbehörde (Art. 31, Art. 36 DSGVO):** Er arbeitet mit der für den Verantwortlichen zuständigen Aufsichtsbehörde zusammen — bei öffentlichen Stellen regelmäßig der oder dem Landesbeauftragten für den Datenschutz — und unterstützt bei der Vorabkonsultation. **Wendet sich eine Aufsichtsbehörde wegen einer Verarbeitung für den Verantwortlichen an ihn, unterrichtet er diesen unverzüglich**, soweit ihm das nicht untersagt ist, und stimmt die Antwort mit ihm ab.

(6) Die Leistungen nach Abs. 3–5 erbringt er binnen **zehn Arbeitstagen** nach Zugang der Anfrage, im Zusammenhang mit einer Meldung nach Art. 33 DSGVO unverzüglich. Für Fristhindernis, Vergütung, Freikontingent und Obergrenze gilt § 5 Abs. 3 entsprechend.

§ 7 Löschung und Rückgabe nach Vertragsende (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

(1) **Wahlrecht:** Nach Beendigung des Hauptvertrags — gleich aus welchem Grund — kann der Verantwortliche verlangen:

a) **Rückgabe** aller personenbezogenen Daten nach Art. 28 Abs. 3 Satz 2 lit. g DSGVO in Format und Umfang des Absatzes 3; danach löscht der Auftragsverarbeiter sie und alle bei ihm vorhandenen Kopien nach den Absätzen 4 und 5, oder
b) **Löschung** aller personenbezogenen Daten einschließlich etwaiger Kopien, oder

c) eine **Kombination** aus Rückgabe bestimmter Kategorien und Löschung der übrigen; für die zurückgegebenen gilt Buchstabe a.

(2) **Frist und Default-Regel außerhalb eines Anbieterwechsels:** Der Verantwortliche teilt seine Wahl spätestens 30 Tage nach Beendigung mit; der Auftragsverarbeiter führt sie binnen 30 Tagen nach Weisung aus. Erfolgt trotz Erinnerung keine Wahl, löscht er nach Fristablauf datenschutzkonform; gesetzliche Aufbewahrungspflichten bleiben unberührt. **Ist der Verantwortliche eine öffentliche Stelle mit archivrechtlicher Anbietungspflicht, ruht die Löschung auf seine Mitteilung in Textform**, bis er die Unterlagen dem zuständigen Archiv angeboten hat und über die Übernahme entschieden ist; den Abschluss teilt er unverzüglich mit. Ohne diese Mitteilung löscht der Auftragsverarbeiter nach Fristablauf — aus den Daten ist eine Anbietungspflicht nicht erkennbar. **Im Anwendungsbereich des Anbieterwechsels gilt ausschließlich Abs. 2a.**

(2a) **Verhältnis zum Anbieterwechsel nach der Verordnung (EU) 2023/2854:** Soweit die Leistung ein Datenverarbeitungsdienst im Sinne des Art. 2 Nr. 8 ist, kann der Verantwortliche mit höchstens zwei Monaten Ankündigungsfrist Wechsel, Überführung auf eigene IT-Infrastruktur oder Löschung verlangen (Art. 23 Buchst. a, Art. 25 Abs. 2 Buchst. d). Danach läuft ein Übergangszeitraum von höchstens 30 Kalendertagen; der Vertrag gilt fort, der Auftragsverarbeiter unterstützt den Wechsel und erhält die geschuldeten Funktionen aufrecht (Art. 25 Abs. 2 Buchst. a, Abs. 3). Ist der Wechsel darin technisch nicht durchführbar, begründet er das binnen 14 Arbeitstagen und benennt einen alternativen Zeitraum von höchstens sieben Monaten. Bei erfolgreichem Wechsel endet der Vertrag mit Benachrichtigung des Verantwortlichen (Art. 25 Abs. 2 Buchst. c), bei reiner Löschwahl mit Ablauf der Ankündigungsfrist; danach bleiben exportierbare Daten und digitale Vermögenswerte mindestens 30 Kalendertage oder für eine vereinbarte Frist abrufbar (Art. 25 Abs. 2 Buchst. g) und werden erst dann vollständig gelöscht. **Ein gescheiterter Wechsel oder der bloße Ablauf des Übergangszeitraums löst weder Vertragsende noch automatische Löschung aus.** Die Datenkategorien ergeben sich aus Ziff. 4 der Präambel.

(3) **Format und Umfang der Rückgabe:** Der Auftragsverarbeiter stellt für sämtliche Anwendungen der Suite einen strukturierten Gesamtexport in einem gängigen, maschinenlesbaren Format bereit; **die Bereitstellung erfolgt entgeltfrei.** Formate je Anwendung: AI Chat als JSON (Konversationen, Nachrichten, Ordner, Binärdateien einschließlich Modell-, Token-, Laufzeit- und Kostenmetadaten); Kalender als JSON bzw. ICS; Kontakte als JSON bzw. VCF einschließlich Gruppen, benutzerdefinierter Felder, Beziehungen und Aktivitätsverlauf; Notizen, Aufgaben und Listen als JSON einschließlich Kommentaren, Anhängen, Tags und Zuordnungen; Mail ordnerweise als MBOX und einzelne Nachrichten als EML; Drive als Einzeldateien im Ursprungsformat bzw. Ordner-ZIP. Die Aufzählung ist nicht abschließend und erfasst auch die Bestände der Anmeldung, des Hubs und der Statusseite. **Bereitgestellt werden die im Arbeitsbereich gespeicherten Bestände einschließlich der Inhalte hochgeladener Dateien**; eine Selbstbedienungsfunktion gibt sie aus, gebunden an die Eigentümerin oder die Verwaltung des Arbeitsbereichs (§ 5 Abs. 1).

Enthalten sind auch die Konfigurationsbestände des Arbeitsbereichs: die strukturierten Konten-, Ordner-, Filter- und Vorlagenangaben des Mail-Moduls — die Nachrichten selbst werden als MBOX und EML ausgegeben —, die **Wissensbestände einschließlich der Wissensdateien, Erinnerungen, Werkzeug-, Widget- und Webhook-Konfigurationen, Vektorbestände und Mailvorlagen des KI-Dienstes** sowie die **Agenten, Anrufe, Prompt-Bausteine, Kanal-Prompts, Benachrichtigungsregeln, Widgets, Widget-Sitzungen und Matrix-Bindungen** der Automations-Anwendung; ausgegeben wird als JSON, jeweils ohne Zugangsgeheimnisse. **Für einen Sprachagenten ist das der Unterschied zwischen Mitnehmen und Neuaufbau; deshalb ist es hier ausdrücklich benannt und nicht nur einer Anlage überlassen.**

Nicht enthalten sind: die Mediendateien zu Messenger-Nachrichten, die auf dem Messenger-Server und nicht im Objektspeicher liegen — sie sind im Abzug benannt, aber nicht mitgeliefert —, die Abläufe der Automations-Anwendung (Definitionen und Fassungen, Ausführungen samt Ein- und Ausgabedaten, Ablaufgedächtnis) sowie Guthaben, Buchungen und Zahlungsereignisse des Arbeitsbereichs. **Diese Bestände stellt der Auftragsverarbeiter auf**

Anforderung bereit — innerhalb der Frist des § 5 Abs. 3, entgeltfrei und mit Nachweis nach Absatz 7 — und **nimmt sie bis zum 31.12.2026 in den strukturierten Abzug auf**; für diesen Termin gelten Mitteilungspflicht und außerordentliches Kündigungsrecht des § 3 Abs. 1 entsprechend. **Den jeweils ausgelieferten Umfang teilt er auf Verlangen in Textform mit.**

(4) **Backups:** Sicherungskopien werden spätestens **90 Tage** nach Rückgabe oder Löschung endgültig und unwiederbringlich gelöscht.

(5) **Löschverfahren:** Gelöscht wird durch endgültiges Entfernen der Datensätze aus der Produktivdatenbank und der Objekte aus dem Objektspeicher; Verweise, Suchindizes und Zwischenspeicher werden mitgelöscht. Sicherungsgenerationen laufen nach Absatz 4 aus; in bestehende Sicherungen wird nicht gezielt eingegriffen. **Physische Datenträgervernichtung (DIN 66399) und Datenträgerbereinigung (NIST SP 800-88) liegen nicht in seiner Verfügungsgewalt** — verarbeitet wird auf angemieteter Rechenzentrumsinfrastruktur; insoweit gelten die Verfahren des in Anlage 3 genannten Betreibers. Seine Sub-Auftragsverarbeiter weist er nach § 4 Abs. 4 zur Löschung an und legt deren Nachweise auf Verlangen vor.

Bestände, die weder eine Löschung durch den Nutzer noch ein zeitgesteuerter Lauf erreicht, weist Anlage 2 als Löschlücken aus — mindestens Dateien im Objektspeicher, die keinem Eintrag mehr zugeordnet sind; die Aufzählung ist nicht abschließend, maßgeblich ist der Nachweisstand in Anlage 2. **Nicht dazu gehören die im AI Chat erzeugten Bilder:** Sie werden mit der Nachricht entfernt, im Übrigen mit der Löschung des Kontos — **soweit der zugehörige Arbeitsbereich noch besteht**; sonst ist die Entfernung gesondert zu veranlassen. Für die Löschlücken löscht er auf Verlangen **manuell** und weist das nach Absatz 7 nach; die automatischen Läufe stellt er bis zum **31.12.2026** her. Die Frist nach Absatz 2 bleibt unberührt.

(6) **Gesetzliche Aufbewahrungspflichten:** Unterliegt der **Auftragsverarbeiter** für einzelne Daten einer eigenen Aufbewahrungspflicht nach Unions- oder mitgliedstaatlichem Recht, nennt er Vorschrift und betroffene Daten vor der Löschung; diese Daten werden bis zum Fristablauf gesperrt, also von der aktiven Verarbeitung ausgeschlossen, und danach unverzüglich gelöscht. **Aufbewahrungspflichten des Verantwortlichen erfüllt dieser selbst; sie berechtigen den Auftragsverarbeiter nicht, die Löschung zu verweigern.**

(7) **Protokoll:** Nach Abschluss der Löschung oder Rückgabe erstellt der Auftragsverarbeiter ein schriftliches Protokoll mit Datum, angewandter Methode und verantwortlicher Person (Name/Funktion), bei Rückgabe zusätzlich dem ausgelieferten Umfang, und übermittelt es binnen 14 Tagen. Es weist ferner die Löschbestätigung der Sub-Auftragsverarbeiter oder den Verweis auf deren Nachweis aus; auf Verlangen legt er diese Nachweise vor.

§ 8 Audit- und Kontrollrechte (Art. 28 Abs. 3 Satz 2 lit. h DSGVO)

(1) **Informationsrecht:** Der Auftragsverarbeiter stellt alle zum Nachweis der Einhaltung dieses AVV erforderlichen Informationen zur Verfügung: Dokumentationen, das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO, soweit es Verarbeitungen für den Verantwortlichen betrifft, das Weisungsregister, TOM-Nachweise, Vertraulichkeitserklärungen — soweit nach § 2 Abs. 2 vorhanden — und das Verzeichnis behördlicher Herausgabeverlangen nach § 1 Abs. 6. **Er weist auf Verlangen ferner nach, welchem Vertragstext eine im Zustimmungsprotokoll geführte Fassungsbezeichnung entspricht. Auf Verlangen legt er für einen einzelnen Empfänger die bestehenden Garantien nach Kapitel V DSGVO und den Vertrag nach Art. 28 DSGVO vor, soweit sie ihm vorliegen und ihre Weitergabe zulässig ist. Eine Vollständigkeit dieser Nachweise über alle Empfänger sagt er nicht zu**; welcher Empfänger einen Mechanismus, einen Vertrag nach Art. 28 DSGVO und eine vollständige Kette führt und welcher nicht, weist Anlage 3 je Zeile aus (§ 4 Abs. 5).

(2) **Kontrollrechte:** Der Verantwortliche oder ein von ihm beauftragter Prüfer (z. B. Datenschutzbeauftragter, Wirtschaftsprüfer, zertifizierter Datenschutzauditor; **bei öffentlichen Stellen auch die nach ihrem Recht zuständige örtliche und überörtliche Rechnungsprüfung, die dafür keiner Beauftragung durch den Verantwortlichen**

bedarf) kann die Einhaltung dieses AVV durch Vor-Ort-Prüfungen, Dokumentensichtungen oder Fragebogen kontrollieren; der Auftragsverarbeiter gewährt dazu Zutritt zu seinen Geschäftsräumen und Einsicht in die dort geführten Nachweise. **Die Rechenzentren stehen nicht in seiner Verfügungsgewalt** (§ 7 Abs. 5); für sie beschafft er die Prüfnachweise des in Anlage 3 genannten Betreibers und legt sie vor, verweigert dieser sie, teilt er das in Textform mit.

(3) **Ankündigung und Frequenz:** Audits sind mindestens **4 Wochen** im Voraus in Textform anzukündigen und auf das erforderliche Maß zu beschränken; nach einem sicherheitsrelevanten Ereignis oder einer Verletzung des Schutzes personenbezogener Daten verkürzt sich die Frist auf **5 Werktage**. Regelmäßig genügt **ein Audit je Kalenderjahr**; weitergehende Prüfungen bleiben zulässig, soweit sie für die Pflichten des Verantwortlichen erforderlich sind — insbesondere in den vorgenannten Fällen oder bei konkreten Anhaltspunkten für einen Verstoß. **Die Befugnisse der Aufsichtsbehörden nach Art. 58 DSGVO bleiben unberührt**; Ankündigungsfrist und Häufigkeitsgrenze gelten für sie nicht.

(4) **Kostenträger:** Für ein reguläres Audit je Kalenderjahr stellt der Auftragsverarbeiter Auskünfte nach Absatz 1 und Nachweise nach Anlage 2 kostenfrei bereit — gleich, ob der Verantwortliche selbst oder ein beauftragter Prüfer es durchführt. Für Vorbereitung und Begleitung einer Vor-Ort-Prüfung kann er eine angemessene Vergütung nach dem Maßstab des § 5 Abs. 3 verlangen; die ersten **vier Stunden je Vertragsjahr** sind eingeschlossen. Bei zusätzlichen Anlassaudits trägt der Verantwortliche die Mehrkosten nach Aufwand — nicht jedoch, wenn der Anlass eine Verletzung des Schutzes personenbezogener Daten, ein sicherheitsrelevantes Ereignis oder ein Verstoß gegen diesen AVV im Verantwortungsbereich des Auftragsverarbeiters ist.

(5) **Nachweisersatz:** Eine externe Zertifizierung oder Testierung schuldet der Auftragsverarbeiter nicht. Erwirbt er eine anerkannte Zertifizierung oder ein Testat (z. B. ISO 27001, SOC 2, BSI C5), legt er den vollständigen Prüfbericht auf Verlangen vor; er ersetzt eine Prüfung nach Absatz 2, soweit er den benannten Prüfgegenstand nachweislich abdeckt und bei Vorlage nicht älter als zwölf Monate ist. Für nicht abgedeckte Prüfgegenstände und bei begründeten Zweifeln an seiner Aussagekraft bleibt die Vor-Ort-Prüfung unberührt; bis zur Vorlage erfolgt der Nachweis über Anlage 2 und Auskünfte nach Absatz 1.

§ 9 Haftung

(1) Jede Partei haftet der anderen für Schäden aus Verstößen gegen diesen AVV nach den allgemeinen gesetzlichen Bestimmungen, soweit nachfolgend nichts anderes gilt.

(2) Für einfache Fahrlässigkeit haftet der Auftragsverarbeiter nur bei Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht), begrenzt auf den bei Vertragsschluss typischerweise vorhersehbaren Schaden; im Übrigen ist sie ausgeschlossen. Ergänzend ist sie begrenzt auf die im Hauptvertrag für das jeweilige Vertragsjahr gezahlte Vergütung, mindestens 5.000 EUR; **gegenüber Verantwortlichen, die juristische Personen des öffentlichen Rechts oder öffentlich-rechtliche Sondervermögen sind, mindestens 25.000 EUR.** Die Grenze gilt für alle Schadensfälle eines Vertragsjahres zusammen. **Der Mindestbetrag greift auch dann, wenn im Vertragsjahr keine Vergütung gezahlt wurde** — etwa in einem entgeltfreien Zeitraum oder einer Freiminutenphase; er ist dann der Höchstbetrag. **Denselben Mindestbetrag bestimmen für öffentliche Stellen § H.1 Abs. 2 des Rahmenvertrags und § 5 Abs. 2a der AGB**; welches Regelwerk die Leistung trägt, ist für seine Höhe deshalb ohne Bedeutung. **Ein höherer Höchstbetrag kann im Hauptvertrag oder im Leistungsschein vereinbart werden. Gegenüber Verantwortlichen, die Verbraucher (§ 13 BGB) sind, gilt diese betragsmäßige Begrenzung nicht.** Die Parteien gehen davon aus, dass dieser Betrag den typischerweise vorhersehbaren Schaden abdeckt; der Nachweis eines höheren bleibt dem Verantwortlichen unbenommen. **Der Betrag ist damit eine widerlegliche Vermutung des typischerweise vorhersehbaren Schadens und keine absolute Obergrenze. Diese Begrenzungen gelten allein im Verhältnis der Parteien zueinander; gegenüber betroffenen Personen gelten sie nicht (Absatz 3).** Die Haftungsbeschränkungen gelten **nicht** bei Vorsatz oder grober Fahrlässigkeit, für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, für

Ansprüche nach dem Produkthaftungsgesetz, bei arglistig verschwiegenen Mängeln, für zugesicherte Eigenschaften und die Übernahme einer Garantie sowie für den Rückgriff nach Art. 82 Abs. 5 DSGVO. **Termine und Zeitangaben, die dieser Vertrag oder Anlage 2 und 3 für die Umsetzung offener Maßnahmen nennen, sind keine Zusicherung einer Eigenschaft und keine Garantie im Sinne des vorstehenden Satzes.**

Offen und deshalb hier bezeichnet: das Verhältnis zu § 4 Abs. 4. Dort haftet der Auftragsverarbeiter für Pflichtverletzungen eines Sub-Auftragsverarbeiters nach Art. 28 Abs. 4 Satz 2 DSGVO **in vollem Umfang**, während dieser Absatz die Haftung für einfache Fahrlässigkeit der Höhe nach begrenzt. **Ob und wieweit die Begrenzung jene Haftung erfasst, legen die Parteien mit diesem Vertrag nicht fest**; die Frage ist einer gesonderten Vereinbarung vorbehalten. Bis dahin bleiben die gesetzlichen Auslegungsregeln unberührt, und die Außenhaftung nach Absatz 3 sowie der Rückgriff nach Art. 82 Abs. 5 DSGVO sind von der Begrenzung ohnehin ausgenommen.

(3) Gegenüber betroffenen Personen haften Verantwortlicher und Auftragsverarbeiter, soweit beide an derselben Verarbeitung beteiligt und für den Schaden verantwortlich sind, nach Art. 82 Abs. 4 DSGVO **als Gesamtschuldner auf den gesamten Schaden**; der Auftragsverarbeiter unter den Voraussetzungen des Art. 82 Abs. 2 Satz 2 DSGVO. Wer den vollständigen Schadensersatz geleistet hat, kann von der anderen Partei den ihrem Verantwortungsanteil entsprechenden Teil ersetzt verlangen (Art. 82 Abs. 5 DSGVO); Art. 82 Abs. 3 DSGVO bleibt unberührt.

(4) **Übermittlung in ein Drittland auf Weisung (§ 4 Abs. 5).** Dieser Absatz gilt nur gegenüber Verantwortlichen, die Unternehmer (§ 14 BGB) oder öffentliche Stellen sind; **gegenüber Verbrauchern ist er nicht vereinbart.**

a) **Pflichten des Verantwortlichen.** Erteilt der Verantwortliche eine Drittland-Weisung, ist er verpflichtet, dafür zu sorgen, dass für die Verarbeitung der übermittelten Daten eine Rechtsgrundlage besteht; die betroffenen Personen über die Übermittlung und ihren Empfänger zu unterrichten (Art. 13 Abs. 1 lit. f, Art. 14 Abs. 1 lit. f DSGVO); besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) nur nach eigener Prüfung übermitteln zu lassen; und als Behörde in Ausübung hoheitlicher Befugnisse nur Empfänger zu wählen, die ihm nach § 1 Abs. 8 zur Verfügung stehen. Das Prüfergebnis, das Anlage 3 für den Empfänger ausweist, zeigt ihm der Auftragsverarbeiter vor der Weisung an (§ 4 Abs. 5); über den Einsatz entscheidet der Verantwortliche.

b) **Freistellung.** Nimmt ein Dritter — insbesondere eine betroffene Person — den Auftragsverarbeiter wegen einer Übermittlung in Anspruch, die auf einer Drittland-Weisung beruht und die der Auftragsverarbeiter weisungsgemäß und unter Einhaltung seiner eigenen Pflichten aus diesem Vertrag ausgeführt hat, stellt ihn der Verantwortliche von dem Anspruch und den angemessenen Kosten der Rechtsverteidigung frei. Voraussetzung ist, dass der Auftragsverarbeiter ihn unverzüglich unterrichtet, den Anspruch nicht ohne seine Zustimmung anerkennt und ihm die Abwehr überlässt, soweit das rechtlich möglich ist. **Die Freistellung entfällt, soweit der Auftragsverarbeiter den Anspruch durch eine Verletzung eigener Pflichten mitverursacht hat** (§ 254 BGB entsprechend); **für Geldbußen, die gegen den Auftragsverarbeiter wegen eigener Verstöße verhängt werden, gilt sie nicht.** Gegenüber einer öffentlichen Stelle ist die Freistellung der Höhe nach auf den Höchstbetrag nach Absatz 2 begrenzt; eine der Höhe nach unbestimmte Verbindlichkeit kann sie ohne Veranschlagung nicht eingehen (ebenso Absatz 4 der Anlage KI-VO des Rahmenvertrags).

c) **Haftung.** Für Schäden, die allein daraus entstehen, dass die Rechtsordnung des Drittlands kein im Wesentlichen gleichwertiges Schutzniveau gewährleistet — insbesondere aus dem Zugriff dortiger Behörden —, haftet der Auftragsverarbeiter dem Verantwortlichen nicht; dieses Risiko hat der Verantwortliche mit der Weisung in Kenntnis des Prüfergebnisses gewählt. **Satz 1 gilt nicht, soweit der Auftragsverarbeiter oder ein Unteranbieter eine eigene Pflicht verletzt hat, und nicht in den Fällen, für die Absatz 2 die Haftungsbeschränkungen ausschließt** (Vorsatz, grobe Fahrlässigkeit, Verletzung von Leben, Körper oder Gesundheit, Produkthaftungsgesetz, Garantie). Im Übrigen bleibt es bei den Absätzen 1 und 2; die Haftung für Unteranbieter nach § 4 Abs. 4 berührt dieser Buchstabe nicht.

d) **Was dieser Absatz nicht leistet.** Er wirkt nur zwischen den Parteien. Gegenüber betroffenen Personen haften beide nach Absatz 3 — der Auftragsverarbeiter nach Art. 82 Abs. 2 Satz 2 DSGVO nur, wenn er seine eigenen Pflichten

verletzt oder außerhalb oder entgegen der Weisung gehandelt hat. Die Aufsichtsbehörde bindet er nicht; eine Geldbuße wegen eigener Verstöße trägt jede Partei selbst. **Der Schutz des Auftragsverarbeiters hängt deshalb daran, dass Weisung, Sperre und Protokoll nach § 4 Abs. 5 und 5b tatsächlich so arbeiten, wie sie beschrieben sind** — nicht an diesem Absatz.

§ 10 Schlussbestimmungen

(1) **Vorrang:** In datenschutzrechtlichen Regelungen geht dieser AVV dem Hauptvertrag vor. Zwischen Hauptteil und Anlage geht die Anlage vor, soweit sie Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Datenkategorien, die Kategorien betroffener Personen, die TOM, die Empfänger oder den vereinbarten Leistungsumfang konkret beschreibt (Anlagen 1 bis 5); im Übrigen der Hauptteil. **Ausgenommen vom Vorrang der Anlagen sind sämtliche im Hauptteil vereinbarten Fristen, Sperren und Leistungspflichten, insbesondere die der §§ 1, 3, 4, 5, 6 und 7.** Beschreibt eine Anlage eine Lücke in den Maßnahmen oder einen abweichenden Einsatz eines Empfängers, ist das eine Beschreibung des Ist-Zustands und **keine Einschränkung der geschuldeten Pflichten und keine Genehmigung**; der Auftragsverarbeiter schuldet sie unverändert und schließt die Lücke zu den in der Anlage genannten Terminen.

(2) **Textform:** Änderungen und Ergänzungen dieses AVV bedürfen der Textform.

(3) **Anwendbares Recht und Gerichtsstand:** Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts (CISG); ist der Verantwortliche Verbraucher (§ 13 BGB), bleiben zwingende verbraucherschützende Vorschriften seines gewöhnlichen Aufenthaltsstaats unberührt. Ausschließlicher Gerichtsstand ist Neuruppin, sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist (§ 38 ZPO); **ist er juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, können die Parteien stattdessen seinen Sitz vereinbaren.** Gegenüber Verbrauchern gilt der gesetzliche Gerichtsstand; der Auftragsverarbeiter kann sie nur vor den Gerichten ihres Wohnsitzstaates verklagen (Art. 18 Abs. 2 der Verordnung (EU) Nr. 1215/2012).

(4) **Unwirksame Bestimmungen:** Ist eine Bestimmung ganz oder teilweise unwirksam oder undurchführbar, bleiben die übrigen unberührt; an ihre Stelle treten die gesetzlichen Vorschriften (§ 306 Abs. 2 BGB). Weitergehende Lücken werden durch ergänzende Vertragsauslegung geschlossen.

(5) **Übertragung.** Die Übertragung dieses AVV oder der Auftragsverarbeitung auf einen Dritten bedarf der vorherigen Zustimmung des Verantwortlichen in Textform (Art. 28 Abs. 1 DSGVO); das gilt auch bei Veräußerung des Geschäftsbetriebs oder eines Betriebsteils, bei Umwandlung und bei einem Gesellschafterwechsel, der die Kontrolle über den Auftragsverarbeiter ändert. **§ S.5a des Rahmenvertrags gilt insoweit nicht. Ohne diese Zustimmung ist auch die Übertragung des Hauptvertrags ausgeschlossen** (§ S.5a Satz 4 des Rahmenvertrags) — sonst fielen Hauptvertrag und dieser Vertrag auseinander, und der Verantwortliche dürfte den Dienst nach § 6 Abs. 1 des Rahmenvertrags nicht weiter nutzen. Die Zustimmung darf nicht wider Treu und Glauben verweigert werden; wird sie verweigert, kann der Verantwortliche diesen AVV und den Hauptvertrag außerordentlich kündigen. § 7 bleibt anwendbar.

Anlage 1: Beschreibung der Verarbeitung

Diese Anlage konkretisiert die Rahmenangaben nach Art. 28 Abs. 3 Satz 2 DSGVO und ist Bestandteil des AVV.

Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Datenkategorien und die Kategorien betroffener Personen ergeben sich aus Ziff. 1 bis 5 der Präambel. **Zur Dauer nach Vertragsende** tritt § 7 hinzu: je bis zu 30 Tage für Wahl und Ausführung (Abs. 2), im Anwendungsbereich des Abs. 2a zusätzlich mindestens 30 Kalendertage Abrufzeit, Sicherungskopien bis 90 Tage nach der Produktivlöschung (Abs. 4); gesetzliche Aufbewahrungspflichten nach Abs. 6 bleiben unberührt. **Die Art der Verarbeitung umfasst die Übermittlung an die in Anlage 3 genannten Empfänger.**

Drittlandtransfers erfolgen nur an vorab mitgeteilte und genehmigte Empfänger, deren Mechanismus und Prüfergebnis Anlage 3 ausweist (§ 4 Abs. 5 und Abs. 6). **Welche Kanäle Gegenstand der Verarbeitung sind, bestimmt Anlage 5; welche Empfänger für sie eingesetzt werden, der Leistungs- und Anbieterschein** — dort wird je Leistung Regelweg oder abweichende Wahl angekreuzt.

Sprachdienste (Voice). Rechtsträger, Verarbeitungsort und Umsetzungsstand je Empfänger führt Anlage 3, die Anbieterfestlegungen § 4 Abs. 6. Das Gesprächsmodell der vom Auftragsverarbeiter selbst und der managed betriebenen Agenten läuft bei einem Anbieter mit Verarbeitung in der Europäischen Union (Anlage 3) — bei Azure OpenAI verarbeiten Ressourcen in Regionen der Europäischen Union und des EWR (Anlage 3, Fußnote 2), ein Verarbeitungsort in einem bestimmten Mitgliedstaat wird nicht zugesichert, und der Beleg der Bereitstellungsart „Datenzone EU“ steht noch aus —, soweit der Verantwortliche in der Anbieterauswahl nichts anderes gewählt hat; für einen selbst angelegten Agenten wählt der Verantwortliche. Eingehende Anrufe führen **Vonage B.V.** (Niederlande) und **Twilio Ireland Limited** (Irland) zu, übermittelt werden Rufnummer, Verbindungsmetadaten und Gesprächston; beide verarbeiten dabei im Auftrag, Anlage 3 führt sie deshalb mit der Rolle *beides*. Welcher der beiden für einen Arbeitsbereich eingesetzt wird, teilt der Auftragsverarbeiter auf Verlangen in Textform mit. Drittlandprovider bleiben wählbar. **Voreinstellung sind sie in den EU-Betriebsarten (Sentinel, Cortex) nirgends. Die Betriebsart Apex** stellt der Auftragsverarbeiter jedem Arbeitsbereich zur Auswahl; sie läuft auf Empfängern in den USA, die Anlage 3 nennt (Festlegung b), und ist nur wählbar, solange der Arbeitsbereich eine wirksame Drittland-Weisung führt — ohne sie ist sie gesperrt. Wählt der Verantwortliche sie, verarbeitet der Auftragsverarbeiter die Eingaben in seinem Auftrag, und die Übermittlung stützt sich wie bei jedem anderen Drittlandmodell auf diese Auswahl als Weisung.

Rückfallebenen — was gilt und was nicht. Ein automatischer Rückfall auf einen Empfänger, den der Verantwortliche nicht gewählt hat, findet nicht statt (§ 4 Abs. 5). **Für Spracherkennung, Gesprächsmodell und Sprachsynthese eines Sprachagenten kann der Verantwortliche jedoch selbst eine Rückfallebene bestimmen**; sie wirkt erst, wenn er sie gesetzt hat, und führt ausschließlich zu dem dort von ihm benannten Empfänger. Setzt er keine, findet kein Rückfall statt. **Benennt er einen Empfänger in einem Drittland, gelten für ihn § 4 Abs. 5 und Abs. 6 unverändert** — die Rückfallebene ist eine Auswahl wie jede andere und ersetzt weder Drittland-Weisung noch Unterrichtung. Für die vom Auftragsverarbeiter selbst und die managed betriebenen Agenten gilt § 4 Abs. 5 letzter Unterabsatz unverändert auch für die Rückfallebene. **Hier stand bis zur Fassung 2.40, einen automatischen Fallback gebe es nicht; das war zu weit gefasst** — die Mechanik besteht, sie steht nur unter der Wahl des Verantwortlichen.

Speicherung von Gesprächstranskripten. Die Funktion ist in der Voreinstellung abgeschaltet (Art. 25 Abs. 2 DSGVO). Aktiviert der Verantwortliche sie, muss er zuvor die Einwilligung des Gesprächspartners einholen und nachweisen; **ist er eine öffentliche Stelle, tritt der nachstehende Absatz an die Stelle dieser Anforderung.** Eine Tonaufnahme im Sinne des § 201 Abs. 1 Nr. 1 StGB findet nicht statt; das Gesprächsaudio wird nur transient verarbeitet (Ziff. 4 der Präambel). Der Auftragsverarbeiter stellt einen Einwilligungsdialog bereit, der zu Gesprächsbeginn abläuft, das Ergebnis zum Anruf speichert und — soweit der Verantwortliche die Optionen nicht abwählt — bei Ablehnung Transkript, Zusammenfassung und Anrufer-Datensatz unterdrückt sowie die Rufnummer hasht. **Bei Sprach-Agenten lässt sich die Transkriptspeicherung nur zusammen mit dem Einwilligungsdialog aktivieren; ohne aktivierten Dialog wird dort kein Transkript gespeichert** — vorbehaltlich des nachstehenden Absatzes. **Für Text- und Chat-Agenten besteht diese Kopplung nicht** — sie führen kein Gespräch, an dessen Beginn ein Dialog ablaufen könnte; für sie stellt der Verantwortliche die Rechtsgrundlage der Speicherung nach § 1 Abs. 1 sicher, und es gelten die Aufbewahrungsfristen der Anlage 2. Eine abweichende Einstellung nimmt er nur auf ausdrückliche Weisung nach § 1 Abs. 2 vor und weist dabei nach § 1 Abs. 4 auf die Rechtsfolgen hin.

Öffentliche Stellen: die Grundlage benennt der Verantwortliche, nicht dieser Vertrag. Ist der Verantwortliche eine öffentliche Stelle, tritt an die Stelle der Einwilligung die von ihm benannte Rechtsgrundlage; er teilt sie dem Auftragsverarbeiter in Textform mit (§ 1 Abs. 2). Der Grund: Zwischen einer Behörde und dem Anrufer besteht ein klares Ungleichgewicht, und eine Einwilligung liefert ihr deshalb nach **Erwägungsgrund 43 DSGVO** regelmäßig keine gültige

Rechtsgrundlage; **Art. 6 Abs. 1 lit. f DSGVO steht ihr nach Art. 6 Abs. 1 Unterabs. 2 DSGVO ohnehin nicht offen.** In Betracht kommen damit regelmäßig **Art. 6 Abs. 1 lit. e DSGVO** in Verbindung mit dem für sie geltenden Fachrecht und, soweit eine Aufbewahrungs- oder Dokumentationspflicht sie trifft, **lit. c**. **Welche Grundlage trägt, beurteilt allein der Verantwortliche** (vgl. § 1 Abs. 7 und Abs. 8); der Auftragsverarbeiter prüft sie nicht, schuldet dazu keine Rechtsberatung und schreibt ihm keine vor. **Mit der Mitteilung richtet er die Transkriptspeicherung für die Arbeitsbereiche dieses Verantwortlichen ohne Einwilligungsdialog ein**; die Kopplung des vorstehenden Absatzes gilt insoweit nicht, für die übrigen Verantwortlichen unverändert fort. **Der Einwilligungsdialog bleibt einer öffentlichen Stelle wählbar** — außerhalb hoheitlicher Tätigkeit kann eine Einwilligung tragen; die Wahl trifft sie, nicht der Auftragsverarbeiter. Stützt sie die Speicherung auf lit. e, entsteht ein **Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO**, auf das sie nach Art. 21 Abs. 4 DSGVO ausdrücklich und von anderen Informationen getrennt hinzuweisen hat; der Auftragsverarbeiter nimmt diesen Hinweis auf Weisung in die Unterrichtung nach dem folgenden Absatz auf.

Ohne Einwilligungsdialog entfällt die Unterrichtung des Anrufers nicht — sie hängt nicht an der Rechtsgrundlage. Für Arbeitsbereiche, in denen die Transkriptspeicherung nach dem vorstehenden Absatz ohne Einwilligungsdialog eingerichtet ist, **hält der Auftragsverarbeiter an dessen Stelle eine Unterrichtung zu Gesprächsbeginn aktiv**: dass das Gespräch als Text gespeichert wird, zu welchem Zweck und für welche Dauer, und wo die Information nach Art. 13 DSGVO vollständig abrufbar ist. **Er schaltet sie für diese Arbeitsbereiche nicht ab; eine entgegenstehende Einstellung in der Anwendung ist keine wirksame Weisung nach § 1 Abs. 2, und er führt sie nicht aus, sondern teilt sie dem Verantwortlichen unverzüglich mit** — wie bei der Ansage nach § 1 Abs. 9. **Der Hinweis auf den KI-Charakter nach § 1 Abs. 9 bleibt unberührt und läuft daneben**; die Entkopplung nach dem vorstehenden Absatz erfasst ihn nicht. Inhalt und Richtigkeit der Information nach Art. 13 DSGVO verantwortet der Verantwortliche; die Angaben dafür stellt der Auftragsverarbeiter nach § 5 Abs. 4 bereit.

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Diese Anlage ergänzt § 3 dieses AVV und dokumentiert die nach Art. 32 DSGVO getroffenen Maßnahmen.

Wir treffen geeignete technische und organisatorische Maßnahmen (Art. 32 DSGVO), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Aufstellung dokumentiert die getroffenen Maßnahmen; als offen bezeichnete Maßnahmen sind noch nicht wirksam, und der Spiegelstrich „Bereiche mit benannten Lücken“ nennt die Punkte, für die eine Beschreibung aussteht.

- **Transportverschlüsselung:** Alle Datenübertragungen sind durchgängig durch TLS 1.2/1.3 (HTTPS) verschlüsselt.
- **Verschlüsselung von Geheimnissen:** Zugangsdaten und Geheimnisse (Provider- und Voice-Credentials) liegen spaltenweise mit AES-256-GCM verschlüsselt (encrypt-on-write). Produktiv- und Testumgebung verwenden **denselben Plattform-Schlüssel**; die Trennung ist als offene Maßnahme geführt. Eine vollständige Datenträger-Verschlüsselung (at rest auf Volume-Ebene) besteht **nicht** und ist als offene Maßnahme geführt; bis dahin tragen Hosting in Deutschland, Transport- und Geheimnis-Verschlüsselung das Schutzniveau.
- **E-Mail-Postfächer:** Betreff und Text angebundener Postfächer werden zur Anzeige und Volltextsuche im Klartext vorgehalten, im Suchfeld der Datenbank und als Rohobjekt im Objektspeicher; ein Aufbewahrungsfenster je Konto lässt sich einstellen. Bei Postfächern, die über die betreibereigene Brücke zur Proton AG angebunden sind, endet die Ende-zu-Ende-Verschlüsselung des Anbieters an der Brücke, die die Nachrichten entschlüsselt. Geschützt sind sie durch Zugriffsbeschränkung, Transportverschlüsselung und die Verschlüsselung der Zugangsdaten; die Datenträger-Verschlüsselung ist, wie vorstehend, als offene Maßnahme geführt.

- **Zugriffskontrollen:** Rollenbasierte Berechtigungen begrenzen den Zugriff auf das erforderliche Minimum (Need-to-know). Zeilenbasierte Zugriffskontrolle (Row Level Security) ist auf allen Tabellen des Anwendungsschemas aktiviert. Sie wirkt gegenüber Zugriffen mit Nutzerkennung; serverseitige Dienstzugriffe nutzen eine privilegierte Datenbankrolle, für die die Mandantentrennung in der Anwendungsschicht durchgesetzt wird. **Die Wirksamkeit dieser Schicht ist nicht flächendeckend belegt:** Am 2026-08-13 wurde in einer Anwendung ein Weg an ihr vorbei festgestellt und am 2026-08-14 geschlossen; die gleichartige Prüfung der übrigen Anwendungen ist als offene Maßnahme geführt. Hochgeladene Nutzerinhalte liegen in zugriffsbeschränkten Speicherbereichen; bewusst öffentlich abrufbar sind ausschließlich Profilbilder.
- **Multi-Faktor-Authentifizierung (MFA):** Eine TOTP-basierte Zwei-Faktor-Authentifizierung ist eingerichtet und in der Produktivumgebung **an jeder Weboberfläche für jedes Konto erzwungen, nicht nur für administrative Zugänge**. Die Erzwingung wirkt in der Middleware und damit bei jedem Seitenaufruf; sie hängt an einer Umgebungsvariablen, die in **allen 18 Produktiv-Apps mit Weboberfläche** gesetzt ist. **Wer an der Oberfläche keinen Faktor hat, kommt nicht durch, sondern wird zur Einrichtung geführt. Über die öffentliche Datenschnittstelle wirkt sie nicht:** Ein mit Passwort allein erlangtes Token liest dort die eigenen Daten, weil keine Zugriffsregel der Datenbank die Authentifizierungsstufe prüft. **Der zweite Faktor schützt damit die Oberfläche, nicht die Daten**; die Erzwingung auf Datenbankebene ist als offene Maßnahme geführt. Der administrative Zugang zum Wirtsystem erfolgt ausschließlich per Schlüsselauthentifizierung ohne Passwort. Ergänzend gelten Passwortregeln (mindestens zehn Zeichen, Groß- und Kleinbuchstaben, Ziffern) und zeitlich begrenzte Sitzungs-Token. Wiederholte Anmeldeversuche werden vor dem Authentifizierungsdienst je Quelladresse begrenzt (zehn je Minute, Stoß von fünf, darüber HTTP 429), gezählt bei Anmeldung, Registrierung und Passwortzurücksetzung, nicht bei der Token-Erneuerung; **für die übrigen API-Routen ist die Begrenzung bestimmt, aber nicht angewandt** und als offene Maßnahme geführt. Bei **Registrierung, Anmeldung und Zurücksetzen des Passworts** ist ein **selbst betriebener** Bot- und Spam-Schutz eingebunden: ein Rechenrätsel (Proof of Work), das im Browser des Besuchers gerechnet wird; Aufgabe und Prüfung stellt unser eigener Authentifizierungsdienst. **Ein externer Anbieter ist daran nicht beteiligt; es wird weder IP-Adresse noch Browserkennung an Dritte übermittelt.** Serverseitig erzwungen ist der Nachweis allein bei der **Registrierung** — dort werden ein fehlender, ein gefälschter und ein wiederverwendeter Nachweis abgewiesen. Bei Anmeldung und Zurücksetzen des Passworts öffnet sich das Gate im Browser selbst, wenn kein Nachweis zustande kommt, damit sich niemand aussperrt; dort trägt der Schutz nicht. **Der Authentifizierungsdienst selbst kann den Nachweis nicht erzwingen** — er kennt allein *hcaptcha* und *turnstile*, das eingesetzte Verfahren lässt sich dort nicht hinterlegen; sein öffentlich erreichbarer Endpunkt */auth/v1/** hängt daneben allein an der Ratenbegrenzung. **Geschützt ist damit die Anwendungsroute, nicht der öffentliche Endpunkt neben ihr.** Wir rechnen ihn deshalb **nur für die Registrierung** als Schutzmaßnahme an; seine Erzwingung an den beiden übrigen Wegen ist als offene Maßnahme geführt.
- **Sicherheitsüberprüfungen:** Wir führen anlassbezogene interne Sicherheitsreviews durch und verfolgen die Befunde mit Status in einem internen Register; externe Penetrationstests durch unabhängige Dritte sind vorgesehen (Zielturnus: jährlich). Der wöchentliche automatisierte Schwachstellen-Scan schlägt seit dem 10.08.2026 fehl; bis zu seiner Instandsetzung wird anlassbezogen geprüft. Die Wirksamkeit sämtlicher Maßnahmen wird mindestens jährlich sowie unverzüglich bei wesentlicher Änderung der Verarbeitung, nach einem Sicherheitsvorfall und nach einer Datenpanne überprüft und bewertet; zusätzlich gehen wir das Register der offenen Maßnahmen quartalsweise (31.03., 30.06., 30.09., 31.12.) Zeile für Zeile auf Status und Fristablauf durch. Datum, Umfang und Feststellungen werden dokumentiert; verantwortlich ist die Geschäftsführung. **Ein dokumentierter Durchgang liegt bislang nicht vor:** Der erste war zum 30.09.2026 vorgesehen; seine Dokumentation steht aus und ist als offene Maßnahme geführt.
- **Aktivitätsprotokoll (Nachvollziehbarkeit von Handlungen in den Anwendungen):** Neben dem Betriebsprotokoll der Eingabekontrolle führt die Anwendung je Arbeitsbereich ein Protokoll der Handlungen in

den Anwendungen: **wer** (Person, Agent, Ablauf oder System), **wann**, in **welcher Anwendung**, **welche Aktion** — aus einem festen Katalog, etwa Nachricht gelesen oder gesendet, Datei heruntergeladen, Termin angelegt — an **welchem Objekt** (nur dessen Kennung), dazu Sitzung, IP-Adresse und Gerätekennung. **Inhalte werden nicht erfasst:** keine Betreffzeilen, Nachrichtentexte, Datei- oder Ordnernamen und keine Eingaben an die KI; Zusatzangaben sind auf Schlüssel aus dem Katalog begrenzt. **Zweck:** Sicherheit, Fehlersuche, Nachweis von Zugriffen und die Auskunft der Person über ihr eigenes Handeln. Einträge können weder Nutzer noch die Dienste der Anwendung ändern oder löschen; entfernt werden sie allein durch den Fristlauf (Fristen: Abschnitt „Aufbewahrungsdauer“ dieser Anlage). **Wer was sieht:** (1) **jede Person** ihr eigenes Protokoll („Meine Aktivität“) samt Export; (2) die Rolle **Inhaber** des Arbeitsbereichs — nicht die Administratoren — nur in geteilten Arbeitsbereichen und nur in der dort eingestellten **Einsichtsstufe**: ab Werk **aus**, Stufe A Kennzahlen des Teams, Stufe B Kennzahlen je Person, Stufe C Einzelhandlungen einer Person (je Abruf höchstens 31 Tage, nicht älter als 90 Tage). IP-Adresse, Gerät und Sitzung sieht der Inhaber in keiner Stufe; Handlungen eines Agenten werden dem Agenten zugerechnet, nicht der auslösenden Person. Das Einschalten verlangt die Bestätigung von Hinweis, Folgenabschätzung und Beteiligung der Beschäftigtenvertretung, wird mit Person und Zeitpunkt gespeichert und den Mitgliedern angezeigt, und jede Einsicht in Daten einer Person wird dieser angezeigt. **Für öffentliche Stellen fragt die Anwendung statt nach dem Betriebsrat nach dem Personalrat:** Stufe A und B nur mit der Angabe „kein Personalrat gebildet“ oder einer Dienstvereinbarung, Stufe C nur mit Dienstvereinbarung; maßgeblich ist das Personalvertretungsrecht des Landes. (3) der **Auftragsverarbeiter** nur über eine Betreibersicht mit zweitem Faktor und Begründung, zur Störungsbeseitigung auf Weisung oder bei einem konkreten Sicherheitsanlass; jede solche Einsicht wird dem Inhaber angezeigt. **Eine Auswertung zur Kontrolle von Leistung oder Verhalten einzelner Personen nimmt der Auftragsverarbeiter nicht vor.** Ein pseudonymisierter Auszug — Kennungen je Arbeitsbereich durch einen Schlüsselhash ersetzt, nur Ereignisse ab 30 Tagen Alter, ohne Konto- und Sicherheitsereignisse — ist technisch angelegt und wird nur auf Weisung des Verantwortlichen erstellt. **Die Protokollierung selbst lässt sich nicht abschalten**, nur die Einsicht.

- **Automationen und KI-Agenten:** Ein Ablauf (Workflow) läuft automatisch nur in einer festen, nummerierten **Version**; Änderungen entstehen als Entwurf und wirken erst, wenn eine neue Version veröffentlicht wird, und Zurücknehmen heißt, eine frühere Version wieder live zu setzen. Den Live-Stand setzt allein eine Datenbankfunktion mit eigener Prüfung; Mitglieder und die Dienste der Anwendung schreiben ihn nicht unmittelbar. Nutzt eine Version ein Postfach oder läuft sie im Namen einer Person, geht sie erst mit deren Zustimmung zu genau dieser Version live; die Zustimmung entfällt mit jeder neuen Version, beim Wechsel des Eigentümers und mit dem Ende der Mitgliedschaft. **Eine Version geht darüber hinaus nur durch eine eigens berechtigte Person live:** Freigeben dürfen allein Inhaber und Administratoren des Arbeitsbereichs; ein Mitglied mit Schreibrecht legt eine Version nur zur Freigabe vor, und die Datenbank erzwingt das bei jedem Wechsel des Live-Stands. **In jedem Firmen- und sonstigen Business-Arbeitsbereich ist das ab Werk eingeschaltet;** Inhaber und Administratoren können es dort ausschalten. **Für Arbeitsbereiche öffentlicher Stellen gilt es zwingend und lässt sich nicht abschalten.** Im persönlichen Arbeitsbereich schaltet die Inhaberin oder der Inhaber selbst live. **Für KI-Agenten gilt dasselbe:** eine geänderte Agenten-Fassung wird vorgelegt und wirkt erst mit der Freigabe. Was beim Einschalten der Pflicht bereits live läuft, bleibt live; ein neuer Agent startet unter der Pflicht ausgeschaltet. Jeder Agent kann nur die ihm zugewiesenen Werkzeuge nutzen. Wirkende Aktionen der KI — Senden, Beantworten, Weiterleiten und Löschen von Nachrichten, Anlegen von Agenten — führt der Server in der Voreinstellung erst nach Bestätigung durch einen Menschen aus; das erzwingt der Server, nicht das Modell. Gegen Fremdsteuerung durch Inhalte Dritter sind lesende Werkzeuge allein durch die Kennzeichnung dieser Inhalte geschützt; die Folgen einer Fremdsteuerung werden begrenzt, ausgeschlossen sind sie nicht. Nutzereigener Programmcode läuft in einer abgeschotteten Umgebung ohne Netzzugang.
- **Hosting in DE-Rechenzentren:** Das Kern-Hosting erfolgt bei der Hetzner Online GmbH in Deutschland.

- **Datensparsamkeit und Löschung:** Wir verarbeiten personenbezogene Daten nur im erforderlichen Umfang. Ein täglicher automatisierter Löschlauf greift nach der gesetzten Frist für Gesprächstranskripte und -Metadaten, Audit- und Systemprotokolle, die Anmeldeprotokolle des Authentifizierungsdienstes, die Fehlerdiagnose-Telemetrie, den Papierkorb von Kontakten, Notizen, Aufgaben und Kalender, Widget-Sitzungen sowie — 90 Tage nach dem letzten Anruf — die anruferbezogenen Datensätze der Sprachagenten. **Ein zweiter täglicher Lauf** erfasst das Gesprächsgedächtnis der Arbeitsabläufe, die Ausführungsprotokolle der Arbeitsabläufe samt ihrer Ein- und Ausgabedaten, die Erinnerungen der KI-Anwendungen und die Nutzungsdatensätze der KI-Infrastruktur — je 90 Tage. **Einträge mit zugehöriger Datei im Objektspeicher** — im Papierkorb von Kontakten, Notizen und Aufgaben sowie der gesamte Papierkorb der Dateiablage und der Immobilien-Anwendung — **räumt ein dritter täglicher Lauf nach 30 Tagen**, zuerst die Dateien, dann den Eintrag; eine Datenbankfunktion kann die Speicher-Schnittstelle nicht aufrufen. Für die übrigen Bestände besteht **kein zeitgesteuerter Löschlauf**; sie werden auf Veranlassung der Nutzerin oder des Nutzers und mit dem Ende des Vertragsverhältnisses gelöscht. **Dass beide Ereignisse jeden Bestand erreichen, ist damit nicht gesagt:** Im Objektspeicher liegen einzelne Dateien, die keinem Eintrag mehr zugeordnet sind und deshalb weder die Nutzerlöschung noch ein Lauf erreicht; sie werden täglich gezählt, ihre automatisierte Löschung ist als offene Maßnahme geführt.
- **Bereiche mit benannten Lücken:** Es gibt **keine Vertretung** des Geschäftsführers — bei seinem Ausfall sind die Fristen aus Art. 33 und Art. 12 Abs. 3 DSGVO nicht sichergestellt; **administrativen Zugang zum Wirtsystem hat allein er**; zwei hinterlegte Schlüssel, die zunächst weiteren Personen zugeordnet waren, gehören zu seinen eigenen Geräten (geklärt am 27.09.2026). Seine schriftliche Verpflichtung nach § 2 Abs. 2 des Auftragsverarbeitungsvertrags liegt noch nicht vor und ist als offene Maßnahme geführt. Der Plattform-Schlüssel hat **keine getrennte Sicherungskopie und kein Rotationsverfahren**. Protokolle werden zentral gesammelt, aber **nicht ausgewertet und nicht gegen Veränderung geschützt**. Für den Patchstand des Wirtsystems und die Vernichtung ausgedienter Datenträger besteht **kein festgelegtes Verfahren**; das Wirtsystem trägt **keinen Schadsoftwareschutz** und bezieht Sicherheitsaktualisierungen **nicht automatisiert**. **Der Paketfilter schützt auch die von der Container-Laufzeit veröffentlichten Ports:** Solcher Verkehr durchläuft die regulären Ketten nicht, sondern eine eigens dafür vorgesehene Sonderkette, und die Regel in dieser Sonderkette gehört zur Maßnahme. **Ihre Einrichtung ist als offene Maßnahme geführt**; bis dahin besteht für die veröffentlichten Ports keine Schranke auf dem Wirtsystem. Die Datenhaltungen sind davon nicht betroffen, sie binden ausschließlich in ihr Containernetz. Nicht festgelegt ist ferner ein **Auswahl- und Kontrollverfahren für Sub-Auftragsverarbeiter** (Art. 28 Abs. 1 DSGVO): Was vertraglich gilt, ist geregelt; wonach ein Anbieter ausgewählt wird, welche Nachweise vor der ersten Übermittlung vorliegen müssen und in welchem Turnus sie wiedervorgelegt werden, ist es nicht. **Für den Sprachkanal sind zwei Ketten nicht erhoben.** Bei der **Zuführung eingehender Anrufe** ist nicht erhoben, ob innerhalb der Unternehmensgruppe des Anbieters in ein Drittland weitergereicht wird; der Vertragspartner sitzt im EWR, Kapitel V ist auf die Übermittlung an ihn nicht anwendbar, und kein Dokument dieses Bestands behauptet eine vertragliche Regelung dieser Kette. Bei der **Sprachsynthese** lautet der abgelegte Vertrag nach Art. 28 DSGVO auf eine andere Gesellschaft als den Empfänger, und dessen eigene Subprozessorenkette ist ebenfalls nicht erhoben. Welche Gesellschaften das sind, nennt Anlage 3; beides ist als offene Maßnahme geführt. **Ohne diesen Satz erfasste die Behebungspflicht des § 3 Abs. 1 gerade den Weg nicht, über den ein Bürgertelefon überhaupt erreichbar ist. Für Arbeitsbereiche öffentlicher Stellen hängt die Durchsetzung an einer Kennzeichnung.** Die Anwendung führt am Arbeitsbereich ein **Merkmal für die Rechtsform des Vertragspartners**, das der Auftragsverarbeiter nach der gemäß Anlage 5 geschlossenen Vereinbarung vor Aufnahme des Betriebs setzt. An ihm setzt die Anwendung durch: die Ansage nach § 1 Abs. 9, die Transkriptspeicherung ohne Einwilligungsdialog samt Unterrichtung nach Anlage 1 und die Abweisung **jedes** Drittland-Anbieters, gleich welche Garantie für ihn besteht. **Ohne Kennzeichnung greift keine der drei Schranken**; die Kennzeichnung ist deshalb eine organisatorische Maßnahme des Auftragsverarbeiters.

- **Verfügbarkeit und Sicherungen:** Die Datenbank wird seit dem 10.07.2026 täglich automatisiert gesichert, der Objektspeicher seit dem 28.07.2026; die Sicherungen laufen auf Infrastruktur in Deutschland und werden 30 Tage vorgehalten. **Der Objektspeicher war vom 13.09.2026 bis zum 21.09.2026 nicht gesichert, obwohl die Läufe Erfolg meldeten**; für diesen Zeitraum besteht kein wiederherstellbarer Stand. Behoben ist das seit dem 22.09.2026 — die Prüfung sieht seither auf den Inhalt des Archivs, nicht auf seine Größe. **Der erste planmäßige Lauf danach, am 23.09.2026, ist abgebrochen und am selben Tag vollständig nachgeholt worden**; die Folgen der Lücke sind als offene Maßnahme geführt. **Der Bestand des Messenger-Servers samt seiner Brücken wird mitgesichert. Seit dem 23.09.2026 liegen die Sicherungen auf einem eigenen Bereich der gespiegelten Datenplatten, getrennt vom Systemlaufwerk, auf dem die Datenbank läuft**; den Objektspeicher tragen dieselben Datenplatten. Vier Einschränkungen sind als offene Maßnahmen geführt: Die Sicherungen liegen im selben Server wie das Produktivsystem, sie sind nicht zusätzlich verschlüsselt, ein fehlgeschlagener Lauf wird nicht nach außen gemeldet, und ein dokumentierter Wiederherstellungstest hat noch nicht stattgefunden. **Die erste hat eine ausdrücklich zu nennende Folge:** Beim physischen Totalverlust des Servers oder beim Ausfall des Standorts gehen die Sicherungen mit unter, beim Ausfall beider Datenplatten zusammen mit dem Objektspeicher; bis zur Ablage außerhalb dieses Servers besteht dafür **keine Wiederherstellungsmöglichkeit**, und die andernorts genannten Zielwerte für Wiederanlaufzeit und Wiederherstellungspunkt (RTO / RPO) gelten **nicht**.

Ergänzende AVV-spezifische Maßnahmen

- **Trennungskontrolle:** Kundendaten werden mandantenfähig und logisch getrennt verarbeitet; die Absicherung beschreibt der vorstehende Baustein unter „Zugriffskontrollen“.
- **Wiederherstellungsziele (Art. 32 Abs. 1 lit. c DSGVO): RPO ≤ 24 Stunden** und **RTO ≤ 8 Stunden** für kritische Verarbeitungen, in **Kalenderstunden**. Sie sind **Zielwerte und keine zugesicherte Eigenschaft** und gelten erst, sobald die Sicherungen verschlüsselt und außerhalb des Servers abgelegt sind, auf dem die Produktivsysteme laufen, und der erste Wiederherstellungstest dokumentiert ist (§ 3 Abs. 1); bei Verlust des Produktivstandorts gelten sie nicht, solange die ausgelagerte Ablage aussteht. Ein ausführbares Wiederherstellungs-Skript besteht; mangels dokumentiertem Test ist seine Wirksamkeit nicht belegt. Künftige Tests werden mit Datum, geprüften Komponenten und Ergebnis dokumentiert. Für Leistungen nach der Anlage Managed Services treten deren Reaktions- und Wiederherstellzeiten (§ 3.2) hinzu, gezählt in Servicezeit-Stunden. Zur Löschung von Backup-Ständen gilt § 7 Abs. 4.
- **Belastbarkeit:** Schutz gegen volumetrische Angriffe auf Infrastrukturebene durch den Rechenzentrumsbetreiber; gespiegelte Datenträger (RAID); automatischer Neustart der Dienste; Ressourcenbegrenzung für kritische Komponenten. Angestrebt wird eine Verfügbarkeit von 99,5 % im Monatsmittel außerhalb geplanter Wartungsfenster. Ein fortlaufender Prüflauf hält die Zustandswechsel der Dienste fest; seine eigenen Ausfälle weist er nicht aus, und den Sprachweg unter einer Rufnummer erfasst er nicht — die gemessenen Werte und diese Grenzen nennt Ziffer 4 des Leistungs- und Anbieterscheins. Verfügbarkeitszusagen richten sich nach der Leistungsanlage des Hauptvertrags.
- **Eingabekontrolle (Protokollierung):** Administrative und sicherheitsrelevante Vorgänge — Anlage, Änderung und Löschung von Konten, Organisationen und Arbeitsbereichen, Einladungen, Rollenänderungen, Vergabe und Widerruf von Zugangsschlüsseln, Änderungen an Sicherheitseinstellungen — werden mit Zeitpunkt, handelnder Person und betroffenem Objekt protokolliert und für die nachstehende Dauer aufbewahrt. **Daneben führt die Anwendung ein Aktivitätsprotokoll**, das Lese- und Schreibvorgänge in den Anwendungen je Person festhält — welche Aktion an welchem Objekt, ohne Inhalte —; Zweck, Einsicht und Grenzen beschreibt der vorstehende Baustein unter „Aktivitätsprotokoll“, die Fristen die nachstehende Tabelle.
- **Weitergabekontrolle:** Übermittlungen an Sub-Auftragsverarbeiter laufen über dokumentierte, transportverschlüsselte Schnittstellen; die Empfänger führt Anlage 3.

- **Regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d DSGVO):** ergänzend zum vorstehenden Baustein werden externe Penetrationstests unabhängiger Dritter mit Datum und Ergebnis dokumentiert; wöchentliche automatisierte Aktualisierungsvorschläge für JavaScript-Abhängigkeiten laufen bisher nur für das gemeinsame Wurzelprojekt der Anwendungen, **für die einzelnen Anwendungen sind sie noch nicht eingerichtet**.
- **Öffentliche Stellen — dedizierte Instanz (Zusage, noch nicht Bestand dieser Anlage):** Echtdaten einer öffentlichen Stelle werden nur auf einer ihr zugeordneten Instanz mit eigenem Server in Deutschland, vollständiger Datenträgerverschlüsselung und verschlüsselter Sicherung außer Haus mit regelmäßigem Wiederherstellungstest verarbeitet; Bereitstellung und Nachweis erfolgen vor Beginn der Echtdatenverarbeitung (§ 3 Abs. 6). **Die vorstehenden Maßnahmen dieser Anlage beschreiben die gemeinsame Plattform und weisen diese Merkmale nicht aus.**

Aufbewahrungsdauer / automatische Löschung (workspace-bezogen vereinbart)

Die automatische Löschung läuft täglich nach Ablauf der gesetzten Frist. Alle Werte dieser Anlage stehen in der nachstehenden Tabelle; sie werden im übrigen Text nicht wiederholt.

Kategorie	Regelwert (ohne abweichende Weisung)	Höchstwert auf Weisung	je Arbeitsbereich konfigurierbar
Audit-/Systemprotokolle	90 Tage	730 Tage	ja
Aktivitätsprotokoll, alle Einträge (auch sicherheitsrelevante)	90 Tage	730 Tage	ja
Aktivitätsprotokoll, IP-Adresse und Gerätekennung	90 Tage, danach aus dem Eintrag entfernt	—	**nein**
Aktivitätsprotokoll, Anmelde- und Sitzungsdaten (Anmeldungen, neue IP-Adresse, neues Gerät)	90 Tage	—	**nein**
Aktivitätsprotokoll, Nachweis der Einsichtsschaltung (wer wann welche Stufe mit welcher Bestätigung eingestellt hat)	bis zur Löschung des Arbeitsbereichs	—	**nein**
Voice-Transkripte	30 Tage	365 Tage	ja
Call-Metadaten	90 Tage	365 Tage	ja
Anruferbezogenes Gedächtnis (Präambel Ziff. 4)	90 Tage ab dem letzten Anruf	nicht bestimmt	ja
Sitzungen der Web-Sprach- und Chat-Widgets, ohne Nachrichtenaustausch	30 Tage	—	**nein**
Sitzungen der Web-Sprach- und Chat-Widgets, mit Nachrichtenaustausch	90 Tage	—	**nein**

Die Einträge des Aktivitätsprotokolls folgen der Frist der Audit-/Systemprotokolle des Arbeitsbereichs: Regelwert 90 Tage, vom Verantwortlichen auf bis zu 730 Tage verlängerbar (die Änderung wird quittiert). IP-Adresse und Gerätekennung sowie die Anmelde- und Sitzungsdaten werden nach 90 Tagen entfernt, und diese 90 Tage sind nicht je Arbeitsbereich einstellbar. Eine **kürzere** Frist als 90 Tage lässt die Konfiguration nicht zu; der Auftragsverarbeiter

setzt sie auf Weisung durch gesonderte Löschung um und bestätigt das in Textform. Das Sichtfenster der Einsicht des Inhabers ist davon unabhängig (höchstens 90 Tage zurück).

Das anruferbezogene Gedächtnis stand hier zuerst nicht — es ist die einzige Kategorie, die einen Anrufer über das einzelne Gespräch hinaus fortschreibt, und ohne seine Frist kann der Verantwortliche weder Art. 30 Abs. 1 lit. f noch Art. 13 Abs. 2 lit. a DSGVO für sie beantworten.

Die Fristen der Widget-Sitzungen gelten auch für Personen ohne Vertragsbeziehung zum Verantwortlichen (Ziff. 5 der Präambel). **Eine abweichende Frist setzt der Auftragsverarbeiter für diese Sitzungen auf Weisung manuell um und bestätigt das in Textform**; die Herstellung der Konfigurierbarkeit ist als offene Maßnahme zum Termin des § 3 Abs. 1 geführt.

Abweichende Vereinbarung: Der Verantwortliche kann die Fristen durch Weisung nach § 1 Abs. 1 bis zum Höchstwert der Tabelle **verlängern**; der Auftragsverarbeiter setzt den gewiesenen Wert im Arbeitsbereich und zeigt die gesetzten Werte auf Verlangen an. **Eine Verkürzung unter die Regelwerte setzt der Auftragsverarbeiter auf Weisung ebenfalls um** (§ 1 Abs. 1), aber nicht über die Konfiguration: Für Audit- und Systemprotokolle, Voice-Transkripte und Call-Metadaten lässt der Arbeitsbereich nur Werte zwischen Regelwert und Höchstwert der Tabelle zu. Die kürzere Frist setzt er deshalb durch gesonderte Löschung der betroffenen Daten nach Ablauf der gewiesenen Frist um und bestätigt das in Textform. **Unberührt bleibt die Löschung einzelner Daten auf Verlangen** (§ 5 Abs. 1, § 7) — die Regelwerte betreffen die Aufbewahrungsfrist, nicht den Einzelfall.

Anlage 3: Empfängerübersicht — genehmigte Sub-Auftragsverarbeiter und Empfänger in eigener Verantwortlichkeit

Diese Anlage ergänzt § 4 dieses AVV. Änderungen werden dem Verantwortlichen gemäß § 4 Abs. 2 mit einer Frist von 30 Tagen vorab mitgeteilt.

Welche Fassung dieser Liste Vertragsbestandteil ist, weist ihr Fußvermerk mit Fassungsnummer und Erhebungsstichtag aus. Maßgeblich ist die Fassung im zugestellten Vertragstext; an ihr misst sich, ob eine spätere Liste den Kreis der Sub-Auftragsverarbeiter ändert und die Mitteilungspflicht nach § 4 Abs. 2 auslöst.

Teil A — sämtliche Empfänger

> **Wie diese Übersicht zu lesen ist. — Stand der Liste: Erhebungsstichtag 2026-10-13.** Sie führt die Empfänger, die für die vereinbarten Leistungen eingesetzt werden oder im Anbieterkatalog zur Auswahl stehen, mit **Rolle, Status und Mechanismus, die für sie gelten** — an ihr erkennt der Auftraggeber die Änderung des Subprozessorenkreises, und daran hängt die Mitteilungspflicht nach § 4 Abs. 2 des Auftragsverarbeitungsvertrags (Art. 28 Abs. 2 und 4 DSGVO). Welche Festlegung für einen Empfänger gilt, steht in der Spalte **Zweck**.
>
> **Was diese Liste ausdrücklich nicht verschweigt:** Fehlt für einen Empfänger eine Garantie nach Kapitel V DSGVO, ein Vertrag nach Art. 28 DSGVO oder eine lückenlose Kette, **steht das in seiner Zeile** — es ist der Inhalt der Zeile und kein Ausschlussgrund. **Für die Empfänger, die über die betreibereigene Automatisierungsplattform erreicht werden, ist die Liste nicht abschließend:** Die Zuordnung der dort eingerichteten Zugänge zu den Leistungen dieser Liste ist noch nicht abgeschlossen. Aufgenommen ist bisher allein die Pinecone Systems, Inc. (Tabelle); einen weiteren Empfänger, der sich bei der Zuordnung ergibt, nehmen wir auf und teilen ihn nach § 4 Abs. 2 des Auftragsverarbeitungsvertrags mit.

Rolle: *AV* Sub-Auftragsverarbeiter nach Art. 28 DSGVO, mit Vertrag zur Auftragsverarbeitung · *eigen* **unsere** eigene Verantwortlichkeit (Art. 4 Nr. 7 DSGVO) · *Dritter* der Empfänger entscheidet über die weitere Verarbeitung als eigener Verantwortlicher; wir sind insoweit weder Verantwortliche noch Auftragsverarbeiterin · *beides* beides, getrennt nach Vorgang · *selbst* von uns selbst auf eigener Infrastruktur betrieben — Verarbeitung im Auftrag, ohne beteiligten eigenständigen Sub-Auftragsverarbeiter · *ohne Vertrag* weder ein Vertrag nach Art. 28 DSGVO noch eine sonstige Vereinbarung; der Empfänger ist kein Sub-Auftragsverarbeiter, Daten fließen nur, soweit die Statusspalte *in Betrieb* ausweist · ***AV · ohne Art.-28-Vertrag*** verarbeitet im Auftrag, ohne dass ein auf ihn lautender Vertrag nach Art. 28 DSGVO vorliegt. **Die allgemeine Genehmigung nach § 4 Abs. 1 des Auftragsverarbeitungsvertrags erfasst ihn wie einen *AV*** — die Pflicht des § 4 Abs. 4 ist für ihn jedoch **nicht erfüllt**, und § 10 Abs. 1 lässt sie unberührt: Der Auftragsverarbeiter schuldet sie unverändert

Status: *in Betrieb* wird tatsächlich eingesetzt, eine Übermittlung findet statt · *eingerichtet, ruht* eingerichtet oder wählbar, derzeit keine Übermittlung · *eingerichtet, nicht in Betrieb* als Anbieter beschlossen, noch nicht in Betrieb; die Funktion erbringt ein anderer Empfänger dieser Liste · *ausgesetzt* die Übermittlung ist angehalten. — **Andere Werte kommen nicht vor.** Die Spalte beschreibt den Einsatz im vereinbarten Leistungsumfang; die geltende Festlegung und die Reichweite unserer Zusicherung stehen in der Zweckspalte derselben Zeile. — **Bei einem Empfänger mit Festlegung (b) beruht *in Betrieb* auf der Begehbarkeit des Wegs, nicht auf einem gemessenen Fluss:** Er ist im Katalog wählbar, und an der Erreichbarkeit — nicht am Fluss eines einzelnen Tages — hängt nach § 4 Abs. 1 AVV die Reichweite der allgemeinen Genehmigung. **Ob in einem bestimmten Arbeitsbereich Daten zu ihm fließen, entscheidet allein dessen Auswahl.**

Drittland-Mechanismus: *EU* Verarbeitung in der EU/im EWR, kein Drittlandtransfer · *EU · Ort offen* Sitz im EWR, Kapitel V DSGVO auf die Übermittlung an ihn nicht anwendbar; ob dahinter eine Weiterübermittlung in ein Drittland steht, benennt die Zweckspalte · *EU · selbst* von uns selbst in Deutschland betrieben · *UK* / *CH* / *DPF* Angemessenheitsbeschluss (Art. 45 DSGVO) für das Vereinigte Königreich, die Schweiz bzw. das EU-U.S. Data Privacy Framework · *SCC* EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO, Durchführungsbeschluss (EU) 2021/914) · *TIA: trägt nicht* unser Transfer-Impact-Assessment bestätigt die Übermittlung nicht — weil es die Tragfähigkeit einer ausgewiesenen Garantie nicht trägt oder weil gar keine Garantie besteht und gleichwohl übermittelt wird · *TIA: ohne abschließendes Ergebnis* die Prüfung ist nicht abschließbar, weil eine ihrer Grundlagen fehlt · ***OFFEN*** kein Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) festgelegt — eine Übermittlung, die im Einzelfall auf eine Ausnahme des Art. 49 DSGVO gestützt wird, benennt die Zweckspalte; ob übermittelt wird, zeigt die Spalte **Status**

Drei Festlegungen, auf die Zeilen der Tabelle verweisen. (a) **Kette nicht abschließend dokumentierbar:** Ein Aggregator ändert den Kreis seiner Unteranbieter einseitig; wir können ihn nicht abschließend benennen und sichern deshalb weder die Weitergabe der Art.-28-Pflichten noch eine lückenlose Kette nach Kapitel V DSGVO zu. Diese Angabe braucht der Verantwortliche vor der Wahl. Ein Prüfergebnis *trägt nicht* führt ebenso zu Ausweisung und Unterrichtung, nie zum Entzug der Wahl — **anders ein fehlender Mechanismus, dafür gilt (c).** (b) **Wählbar, nicht Voreinstellung:** Der Empfänger steht im Katalog zur Auswahl und ist in den EU-Betriebsarten Sentinel und Cortex weder eingestellt noch Rückfallebene. **Weist seine Zeile eine Betriebsart aus, in der er gleichwohl voreingestellt ist, gilt das dort Gesagte** — eine solche Ausnahme wird in der Zeile benannt und nicht in dieser Festlegung verschwiegen. Was aus der Festlegung folgt, steht an einer Stelle und wird hier nicht wiederholt: die **Zusage** für die von uns selbst und die managed betriebenen Agenten in **§ 4 Abs. 6 des Auftragsverarbeitungsvertrags**, die **Rollenübersicht** — wer den Anbieter jeweils auswählt — in **Ziff. 4.4 der Datenschutzerklärung**. **Die Betriebsart „Janeway Apex“ fällt unter diese Festlegung:** Wir stellen sie jedem Arbeitsbereich zur Auswahl; sie läuft auf Anthropic und Perplexity (als Ablauf) sowie auf OpenAI und Cartesia (als Agent), alle USA, und ist nur wählbar, solange der Arbeitsbereich eine wirksame Drittland-Weisung führt — ohne sie ist sie gesperrt. In einem Arbeitsbereich eines Auftraggebers verarbeitet sie dessen Daten in seinem Auftrag, und die Übermittlung stützt sich wie bei jedem anderen Drittlandmodell auf seine Auswahl als Weisung; welche Modelle innerhalb der Betriebsart arbeiten, legen wir fest, die Empfänger nennt diese Anlage. **Ausnahmen in unserem eigenen Betrieb benennen wir:** In unseren eigenen

Arbeitsbereichen nutzen wir Apex selbst; dort sind wir Verantwortliche, und die Wahl ist eine bewusste Entscheidung für unsere eigenen Daten. **In unserer zweiten Betriebsumgebung laufen außerdem eigene Demo- und Prüfagenten teilweise auf OpenAI (Sprachmodell) und Cartesia (Sprachsynthese)**; einige davon sind über Rufnummern und Widgets erreichbar, und wer mit ihnen spricht oder schreibt, dessen Eingaben gehen an diese Anbieter. Daten eines Auftraggebers verarbeiten sie nicht. (c) **Ohne Mechanismus kein Angebot über die Weisung:** Einen Empfänger, der im Auftrag verarbeitet und für den kein Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) besteht — Spalte „Drittland-Mechanismus“ beginnt mit *OFFEN* —, bieten wir über die Weisung des Verantwortlichen **nicht** an. Kapitel V bindet den Auftragsverarbeiter selbst (Art. 44 DSGVO); eine Weisung kann eine fehlende Garantie nicht ersetzen. **Steht eine solche Zeile noch auf *in Betrieb*, ist der Weg noch begehbar und die Umsetzung der Festlegung offen** — die Statusspalte sagt es, und an ihr hängt die Reichweite der Genehmigung nach § 4 Abs. 1 des Auftragsverarbeitungsvertrags. Eine Erklärung nach Art. 49 DSGVO, auch im persönlichen Arbeitsbereich, ersetzt weder den fehlenden Mechanismus noch den fehlenden Vertrag nach Art. 28 DSGVO. **Was die Anwendung gleichwohl zulässt: eine gesonderte Freischaltung je Weg.** Inhaber oder Administratoren — im persönlichen Arbeitsbereich die Person selbst — können genau einen solchen Weg nach einem Hinweis auf die fehlende Grundlage freischalten; die Drittland-Weisung öffnet ihn nicht, und für die Daten von Personen, die den Empfänger nicht wählen, sowie für Arbeitsbereiche öffentlicher Stellen bleibt er gesperrt. **Eine Grundlage nach Kapitel V DSGVO schafft die Freischaltung nicht:** Über einen so geöffneten Weg dürfen keine personenbezogenen Daten übermittelt werden, und der Verantwortliche weist die Personen in seinem Arbeitsbereich entsprechend an. Steht die Zeile auf *eingerichtet, ruht*, setzt der erste Einsatz zudem die Mitteilung nach § 4 Abs. 2 des Auftragsverarbeitungsvertrags voraus (§ 4 Abs. 2a).

Anbieter	Sitz / Region	Zweck	Rolle	Status	Drittland-Mechanismus
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Deutschland	Kern-Hosting der gesamten Infrastruktur (Website, Anwendungen, Datenbank, Objektspeicher, KI-Dienste)[1]	*beides*	*in Betrieb*	*EU*
Microsoft Ireland Operations Limited, 70 Sir John Rogerson's Quay, Dublin, D02 R296, Irland (CRO 256796) — Dienste „Azure AI Speech“ (Region Germany West Central) und „Azure OpenAI“	Irland (EU); Azure AI Speech: Verarbeitung in Deutschland; Azure OpenAI: Ressourcen in Regionen der EU und des EWR[2]	Echtzeit-Spracherkennung und Sprachsynthese (beide Region Germany West Central, Verarbeitung in Deutschland) sowie KI-Sprachmodelle über Azure OpenAI (Ressourcen in neun Regionen der EU und des EWR, ohne Zusage eines bestimmten Mitgliedstaats; der Beleg der Bereitstellungsart „Datenzone EU“ steht noch aus). **Verbindlicher Standard** der Spracherkennung für die vom Auftragsverarbeiter selbst und die managed betriebenen Agenten sowie systemseitige Voreinstellung neuer Agenten[2]	*beides*	*in Betrieb*	*EU · SCC*; Azure-OpenAI-Ressourcen in der Schweiz und im Vereinigten Königreich: *CH / UK*[2]
Microsoft Ireland Operations Limited / Microsoft Corporation — Dienst „Microsoft Graph“	Irland (EU) / USA	**Optionale Schnittstelle**, die der Nutzer selbst einrichtet und verantwortet: Abgleich von Kalender-, Kontakt- und Aufgabendaten mit einem selbst verbundenen Microsoft-Konto, **in beide Richtungen**[2]	*Dritter*	*in Betrieb*	*DPF · SCC*[2]

Microsoft Ireland Operations Limited / Microsoft Corporation — Postfachabruf über IMAP (*outlook.office365.com*, Port 993, TLS)	Irland (EU) / USA	**Optionale Schnittstelle**, die der Nutzer selbst einrichtet: **Vollabruf eines gesamten Postfachs** in die Mail-Anwendung, einschließlich der Daten unbeteiligter Dritter[2]	*Dritter*	*in Betrieb*	*DPF · SCC*[2]
Stripe Payments Europe, Ltd., One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Irland (CRO 513174)	Irland (EU) / USA	Zahlungsabwicklung kostenpflichtiger Abonnements; keine aktiven Zugangsdaten[3]	*eigen*	*eingerichtet, ruht*	*DPF · SCC*[3]
Vonage B.V., Radarweg 29 A, 1043 NX Amsterdam, Niederlande (KVK 34223740)	Niederlande (EU)	Rufnummern und Zuführung eingehender SIP-Anrufe an unseren eigenen Echtzeit-Audio-Server[4]	*beides*	*in Betrieb*	*EU · Ort offen*[4]
Twilio Ireland Limited, 70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Irland (CRO 557454)	Irland (EU)	**Zweiter Telefonieanbieter neben Vonage** — Telefonie und SMS-Versand der Gesellschaft, **Zuführung eingehender Anrufe zu Arbeitsbereichen des Verantwortlichen** und **Versand von Kurznachrichten aus dessen Abläufen und Sprachagenten** (Baustein „SMS senden“). **Unter den Beschränkungen des Teils B wird er nicht eingesetzt**[5]	*beides*	*in Betrieb*	*DPF · SCC*[5]
Proton AG, Route de la Galaise 32, 1228 Plan-les-Ouates, Genf, Schweiz	Schweiz	Betrieb der über unsere selbst betriebene Proton Bridge angebundenen Postfächer sowie **Versand unserer System- und Betreiberpost aus den Anwendungen**. **Ein Vertrag nach Art. 28 DSGVO ist in Abschluss**: Die Proton AG stellt einen Auftragsverarbeitungsvertrag öffentlich bereit, der Nachweis seiner Geltung für unser Konto ist nicht abgelegt; bis dahin ist die Vertragskette nicht belegt[6]	*beides*	*in Betrieb*	*CH*[6]
Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris — RCS Paris 433 115 904	Frankreich (EU)	KI-Sprachmodelle (im Katalog wählbar), Text-Embeddings, Sprache-zu-Text (Whisper) außerhalb des Echtzeit-Sprachpfads[7]	*AV*	*in Betrieb*	*EU*
Mistral AI SAS, 15 rue des Halles, 75001 Paris — RCS Paris 952 418 325	Frankreich (EU)	KI-Modelle (EU-Standardbetrieb: Gesprächsmodell der Betriebsart Sentinel und Rückfallebene der Betriebsart Cortex); Gesprächs-LLM im Voice-Standard; Text-Embeddings	*beides*	*in Betrieb*	*EU*

KugelAudio GmbH-, Amtsgericht Charlottenburg HRB 277989 B	Deutschland, Verarbeitung in der Europäischen Union	Sprachsynthese der Voice-Funktion und deren EU-Standard, in der gesondert gebuchten Variante „EU-Only Hosting“ — **EU-Hosting durch Bestätigung des Anbieters vom 2026-09-23**. **Offen: die Subprozessorenkette und ein auf diese GmbH lautender Vertrag nach Art. 28 DSGVO**[8]	*AV · ohne Art.-2-8-Vertrag*	*in Betrieb*	***EU***[8]
Deepgram, Inc., 548 Market St, Suite 25104, San Francisco, CA 94104-5401, USA	USA	Echtzeit-Spracherkennung. **Wählbar, nicht Voreinstellung** (Festlegung b)[9]	*AV*	*in Betrieb*	*SCC · TIA: trägt nicht*[9]
Eleven Labs Inc., 169 Madison Ave #2484, New York, NY 10016, USA	USA	Sprachsynthese. **Wählbar, nicht Voreinstellung** (Festlegung b)[10]	*AV*	*eingerichtet, ruht*	*DPF · SCC · TIA: trägt nicht*[10]
Cartesia AI, Inc., 555 De Haro Street, Suite 300, San Francisco, CA 94107, USA	USA	Sprachsynthese. **Wählbar, nicht Voreinstellung** (Festlegung b)[11]	*AV*	*in Betrieb*	*SCC · TIA: trägt nicht*[11]
OpenAI, L.L.C. (*OpenAI OpCo, LLC*), 1455 3rd Street, San Francisco, CA 94158, USA	USA	Sprachsynthese, Sprachmodell, Text-Embeddings, Bildgenerierung. **Wählbar, nicht Voreinstellung** (Festlegung b)[12]	*AV*	*in Betrieb*	*SCC · TIA: trägt nicht*[12]
Anthropic PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA	USA	Sprachmodell. **Wählbar, nicht Voreinstellung** (Festlegung b)[13]	*AV*	*in Betrieb*	*SCC · TIA: trägt nicht*[13]
Groq LLC, USA — nur ein Postfach veröffentlicht (P.O. Box 1778, Mountain View, CA 94042)	USA / Vereinigtes Königreich	Sprachmodell. **Wählbar, nicht Voreinstellung** (Festlegung b)[14]	*AV*	*in Betrieb*	*UK · SCC · TIA: trägt nicht*[14]
Perplexity AI, Inc., 115 Sansome Street, Suite 900, San Francisco, CA 94104, USA	USA	Sprachmodell. **Wählbar, nicht Voreinstellung** (Festlegung b)[15]	*AV*	*in Betrieb*	*DPF · SCC · TIA: trägt nicht*[15]

KIE (KIE.AI) — **NEXUSAI SERVICES LLC**, 1500 N Grant St #7370, Denver, CO 80203, USA (Colorado 20241592482, Good Standing)	USA	Bildgenerierungs-Aggregator; leitet den Bild-Prompt modellabhängig an weitere Gesellschaften weiter. **Die Modelle der drei Hersteller mit Verarbeitung in der Volksrepublik China führen wir nicht mehr im Katalog. Kette nicht abschließend dokumentierbar. Für ihn besteht kein Vertrag nach Art. 28 DSGVO. Über die Weisung eines Arbeitsbereichs nicht angeboten; erreichbar nur nach gesonderter Freischaltung je Weg** (Festlegung c)[16]	***AV · ohne Art.-2-8-Vertrag***	*eingerichtet, ruht*	***OFFEN · TIA: trägt nicht***[16]
OpenRouter, Inc., 169 Madison Avenue, New York, NY 10016, USA — Delaware, Register des Staates New York 7543396, Status aktiv	USA	Aggregator für KI-Sprachmodelle; vermittelt die Eingaben des Nutzers an weitere Modellanbieter, deren Kreis er einseitig ändert. **Kette nicht abschließend dokumentierbar. Über die Weisung eines Arbeitsbereichs nicht angeboten** (Festlegung c)[17]	*AV*	*eingerichtet, ruht*	***OFFEN · TIA: trägt nicht***[17]
Pinecone Systems, Inc.-, Vereinigte Staaten — **Anschrift und Registerangaben sind nicht erhoben**	USA	**Vektordatenbank der Wissenssuche eines Telegram-Agenten** im Ablauf eines managed betreuten Kunden auf der betreibereigenen Automatisierungsplattform; übermittelt werden Einbettungen und Auszüge der Gesprächs- und Wissensinhalte[18]	***AV · ohne Art.-2-8-Vertrag***	*eingerichtet, ruht*	***OFFEN***[18]
Linkup Technologies SAS-, 28 avenue des Pépinières, 94260 Fresnes — RCS Créteil 930 910 740	Frankreich (EU)	Web-Suche: **Standard-Backend** der Recherche in den EU-Betriebsarten Sentinel und Cortex, zusätzlich Abruf einzelner Webseiten; auch für die Betriebsart „Janeway Apex“, deren Anfrage an Tavily abgewiesen wird[19]	*AV*	*in Betrieb*	*EU*
AlphaAI Technologies Inc. (Tavily), 1350 Broadway, 24th Floor, New York, NY 10018, USA	USA	Web-Suche. **Über die Weisung eines Arbeitsbereichs nicht angeboten**; ohne gesonderte Freischaltung je Weg wird jeder Aufruf abgewiesen, auch aus der Betriebsart „Janeway Apex“ (Festlegung c). In den EU-Betriebsarten Sentinel und Cortex wird er nicht eingesetzt[20]	*AV*	*eingerichtet, ruht*	***OFFEN · TIA: trägt nicht***[20]
SearXNG (selbst betrieben auf Hetzner)	Deutschland	Web-Suche (Metasuche) als Auffangnetz der EU-Such-Kette hinter Linkup; der Rückfall ist Bestandteil der genehmigten EU-Such-Kette und keine gesonderte Inbetriebnahme	*selbst*	*eingerichtet, ruht*	*EU · selbst*

WhatsApp Ireland Limited	Merrion Road, Dublin 4, D04 X2K5, Irland	Messenger-Modul: Anbindung eines WhatsApp-Kontos über eine selbst betriebene Brücke. **Die Anbindung nimmt der Verantwortliche vor; die Aktivierung ist eine dokumentierte Weisung**[21]	*Dritter*	*in Betrieb*	*EU*
Telegram Messenger Inc. (Vertreter nach Art. 27 DSGVO: European Data Protection Office (EDPO), Avenue Huart Hamoir 71, 1030 Brüssel, Belgien)	Commerce House, Wickhams Cay 1, PO Box 3140, Road Town, Tortola, VG1110, Britische Jungfernins-eln	Messenger-Modul: optionale Anbindung eines eigenen Telegram-Kontos über unsere selbst betriebene Brücke. **Angemessenheitsbeschluss und Garantie nach Art. 46 DSGVO bestehen nicht**; die Nutzung ist auf Einzelvorgänge nach Art. 49 Abs. 1 lit. b DSGVO beschränkt. **Standardmäßig deaktiviert**[22]	*Dritter*	*in Betrieb*	***OFFEN*** · *TIA: trägt nicht* · Art. 49 nur im Einzelfall[22]
CartoDB Inc. (CARTO), 307 Fifth Avenue, Floor 9, New York, NY 10016, USA	USA	Kartenhintergrund der Standortkarte auf der Agentur-Website *janeway-technology.com*-: der Browser verbindet sich unmittelbar mit *basemaps.cartocdn.com* und übermittelt seine IP-Adresse in die USA. **In der Immobilien-Anwendung wird er nicht eingesetzt**[23]	*beides*	*in Betrieb*	*DPF · SCC*[23]
OpenStreetMap Foundation	Vereinigtes Königreich	Immobilien-Anwendung, **zwei Wege mit verschiedenen Daten: Kartenkacheln der Lagekarte** — der Browser lädt sie beim Öffnen eines Objekts mit Koordinaten unmittelbar bei *tile.openstreetmap.org* und **übermittelt dabei seine IP-Adresse**, auch auf der öffentlich abrufbaren Exposé-Seite; **Geocoding (Nominatim)** — Umwandlung einer Objektadresse in Koordinaten, übermittelt wird die Adresse; **dieselbe Schnittstelle löst den Ortsnamen einer Wetterabfrage** des Werkzeugs „Wetter“ der KI-Agenten in Automations auf. **Ohne Vertrag**[24]	*ohne Vertr-ag*	*in Betrieb*	*UK*
TradingView Inc., USA — **Anschrift und Registerangaben sind nicht erhoben**	USA	Kurs-Chart im AI Chat: Öffnet der Nutzer einen solchen Baustein, lädt sein Browser den Chart als eingebetteten Rahmen unmittelbar dort und übermittelt dabei seine IP-Adresse und das abgefragte Kürzel. **Ein Vertrag nach Art. 28 DSGVO besteht nicht und ist für die Rolle *Dritter* auch nicht einschlägig**[25]	*Dritter*	*in Betrieb*	***OFFEN***[25]

onOffice GmbH-, Charlottenburger Allee 5, 52068 Aachen	Deutschland	Immobilien-Anwendung: Anlage von Adress- und Interessentendatensätzen in einem vom Inhaber selbst verbundenen onOffice-Konto — Vor- und Nachname, E-Mail, Telefon und Suchkriterien. Lesen, Ändern und Löschen leistet die Schnittstelle nicht. **Die Verbindung richtet der Verantwortliche ein; die Aktivierung ist seine dokumentierte Weisung**[26]	*AV*	*eingericht-et, ruht*	*EU*
Google LLC · **Mozilla Corporation** · **Microsoft Corporation** · **Apple Inc.** — welcher, ergibt sich aus dem Browser des Nutzers, nicht aus unserer Wahl	USA bzw. EU je nach Dienst	Zustellung der Benachrichtigungen des Messenger-Moduls auf das Gerät des Nutzers, **wenn er sie in seinem Browser erlaubt-**: übermittelt werden die Zustelladresse des Browsers und der verschlüsselte Inhalt[27]	*Dritter*	*eingericht-et, ruht*	*DPF* für Google und Microsoft · *OFFEN* für Mozilla und Apple[27]

Anmerkungen zu den Zeilen

Sie tragen den Inhalt, der bis zur vorigen Fassung dieser Liste in der jeweiligen Tabellenzelle stand, und sind Bestandteil der Zeile, auf die sie verweisen.

[1] **Hetzner.** Den darauf laufenden Supabase-Stack, den Echtzeit-Audio-Server der KI-Telefonie (LiveKit), das interne KI-Gateway, den Dokumentenserver der Dokumentenbearbeitung (OnlyOffice Docs) und den Server des Messengers (Matrix) betreiben wir selbst; sie sind weder eigenständige Sub-Auftragsverarbeiter noch Empfänger.

[2] **Microsoft — gemeinsam für die drei vorstehenden Zeilen.** Geschäftsanschrift der irischen Gesellschaft: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18; Konzernmutter ist die **Microsoft Corporation**, Redmond, WA, USA. — **Azure AI Speech und Azure OpenAI:** Für die Echtzeit-Spracherkennung besteht derzeit **kein Anbieter mit Verarbeitung in der Europäischen Union außer diesem**; der einzige andere wählbare verarbeitet in den Vereinigten Staaten (Deepgram). Für einen selbst angelegten Agenten wählt der Verantwortliche. **Azure AI Speech** verarbeitet in Rechenzentren in Deutschland. **Azure OpenAI betreiben wir mit Ressourcen in neun Regionen der Europäischen Union und des EWR:** Deutschland (Germany West Central), Frankreich (France Central), Irland (North Europe), Italien (Italy North), Niederlande (West Europe), Norwegen (Norway East), Polen (Poland Central), Schweden (Sweden Central) und Spanien (Spain Central). Auf welche dieser Ressourcen eine Anfrage geht, bestimmt die Plattform; **einen Verarbeitungsort in einem bestimmten Mitgliedstaat — auch in Deutschland — sichern wir für das Sprachmodell nicht zu.** Belegt ist der Ort der Ressourcen; der Beleg der Bereitstellungsart „Datenzone EU“ steht noch aus — in der Bereitstellungsart „Global Standard“ könnte der Anbieter die Inferenz in jeder Region ausführen, und die Schnittstelle weist die Bereitstellungsart nicht aus. **Daneben führt der Katalog Azure-OpenAI-Ressourcen in der Schweiz (Switzerland North, Switzerland West) und im Vereinigten Königreich (UK South, UK West).** Für beide Staaten besteht ein Angemessenheitsbeschluss (Art. 45 DSGVO); die Plattform behandelt sie gleichwohl als Drittland-Empfänger: Sie sind nur mit Drittland-Weisung wählbar, weder Voreinstellung noch Rückfallebene der EU-Betriebsarten und für Arbeitsbereiche öffentlicher Stellen gesperrt. Vertragspartnerin ist die Microsoft Ireland Operations Limited mit Sitz im EWR, ein Drittlandtransfer nach Art. 44 DSGVO liegt insoweit nicht vor. Wir stützen die Einbindung ergänzend auf EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO). **Der Angemessenheitsbeschluss ist für diese beiden Dienste nicht Teil der Grundlage:** Ein Eintrag im EU-U.S. Data Privacy Framework wirkt nur zugunsten der zertifizierten US-Organisation und trägt eine Übermittlung an eine irische Gesellschaft nicht; er trägt allein eine Weiterübermittlung an die Microsoft Corporation, deren Umfang offen ist; die Microsoft Corporation ist im Register geführt (Abruf 22.09.2026, *Active – Re-certification under Review*). — **Microsoft Graph:** Termine, Kontakte und Aufgaben des Arbeitsbereichs gehen dabei auch **an** Microsoft. — **Postfachabruf über**

IMAP: Übertragen werden Inhalte, Anhänge, Betreffzeilen sowie Absender- und Empfängeradressen **aller** Nachrichten des Postfachs; Kennzeichnungen und Ordnerbewegungen werden zurückgeschrieben. **Weder vom SMTP-Relay noch von Microsoft Graph gedeckt** — beide erfassen andere Datenarten und einen engeren Umfang. **Diese Zeile beschreibt den Umfang der Schnittstelle, nicht die Anbieterwahl:** Dieselbe Schnittstelle verbindet jeden Postfachanbieter, den der Verantwortliche wählt. **Andere Postfachanbieter bekommen keine eigene Zeile** — sie sind Anbieter des Verantwortlichen, von uns weder ausgewählt noch beauftragt; Microsoft steht hier, weil es auch auf anderen Wegen unser Empfänger ist. — **Für Microsoft Graph und den IMAP-Vollabruf ist der Angemessenheitsbeschluss dagegen einschlägig**, weil dort der Verarbeitungsort das Postfach des Nutzers und damit nicht auf Deutschland festgelegt ist; beide Zeilen führen ihn deshalb. **Wovon es abhängt:** Liegt das verbundene Postfach in den Vereinigten Staaten, ist die Microsoft Corporation unmittelbare Empfängerin — dann trägt der Angemessenheitsbeschluss diese Übermittlung, und seine Fälligkeit ist für sie ein echter Termin. Beide Wege richtet der Nutzer selbst ein und kann sie jederzeit trennen. — **Microsoft Ireland Operations Limited gehört zur Microsoft Corporation (USA) und unterliegt insoweit mittelbar dem US CLOUD Act**; ein Herausgabeverlangen an die Muttergesellschaft kann auch in der EU verarbeitete Daten erfassen. **Gegen einen solchen Zugriff wirkt keine dieser Grundlagen — er ist ein Fall des Art. 48 DSGVO**, gesondert bewertet in unserem Transfer-Impact-Assessment (Ziff. 5.5), das wir dem Auftraggeber auf Verlangen vorlegen. Product Terms und Data Protection Addendum sind noch zur Akte zu nehmen.

[3] **Stripe.** Weiterübermittlung an die Stripe, LLC, South San Francisco, USA. **Vertragspartner und Übermittlungskette sind bis zur Vorlage des Vertrags nicht bestimmt** — die Angabe beruht auf der Anbieterdokumentation und ist vor Inbetriebnahme zu klären.

[4] **Vonage.** Etwaige Weiterübermittlungen in der Unternehmensgruppe (Ericsson AB) sind noch zu erheben und hier auszuweisen. **Im Register des EU-U.S. Data Privacy Framework ist mit der Vonage Holdings Corp., Holmdel, New Jersey, eine Gesellschaft dieser Gruppe in den Vereinigten Staaten geführt** — für die Übermittlung an unseren Vertragspartner im EWR folgt daraus nichts, für die Dringlichkeit der Erhebung sehr wohl.

[5] **Twilio.** Betreiber-Festlegung vom 2026-08-23, für Telefonzentrale **und Suite**. Bei ihm liegen die Hauptrufnummern der Gesellschaft. **Zwei Vorgänge, getrennt zu betrachten:** Telefonie und SMS-Versand der Gesellschaft — dafür sind wir selbst Verantwortliche, einschlägig ist **Modul 2** — und die Zuführung eingehender Anrufe zu Arbeitsbereichen des Verantwortlichen sowie der Versand von Kurznachrichten, die ein Ablauf oder Sprachagent des Verantwortlichen auslöst — übermittelt werden Empfängerrufnummer und Nachrichtentext —, für die er im Auftrag verarbeitet; dafür ist **Modul 3** einschlägig. **Die Drittland-Schranke der Plattform erfasst diesen Weg nicht:** Sie knüpft an den Vertragspartner an, und der sitzt im EWR; die Weiterübermittlung an die Twilio Inc. (USA) tragen die Listung nach dem EU-U.S. Data Privacy Framework und Standardvertragsklauseln (nachstehend), nicht eine Weisung des Arbeitsbereichs. Daraus folgt die Rolle *beides*: Ohne sie dürfte er nach § 4 Abs. 1 des Auftragsverarbeitungsvertrags die Anrufe des Verantwortlichen nicht zuführen, während AGB § 11 Abs. 4 und Anlage 1 sagen, dass er es tut. Welcher der beiden Telefonieanbieter die Rufnummer eines bestimmten Arbeitsbereichs trägt, teilen wir auf Verlangen in Textform mit. **Der Vertragspartner sitzt im EWR; auf die Übermittlung an ihn ist Kapitel V nicht anwendbar. Kapitel V greift für die von ihm ausgewiesene Weiterübermittlung an die Twilio Inc. (USA)** — sie stützt sich auf Standardvertragsklauseln, ergänzt um deren Listung nach dem EU-U.S. Data Privacy Framework; die Rangfolge **DPF, BCR, Standardvertragsklauseln** ist die des Anbieters, nicht unsere Festlegung. **Offen und deshalb hier benannt:** dass der abgelegte Vertrag nach Art. 28 DSGVO und **Modul 3** der Standardvertragsklauseln die Zuführung für Arbeitsbereiche des Verantwortlichen tragen, ist nicht belegt; bis dahin nennt diese Zeile das einschlägige, nicht das nachgewiesene Modul. **Ein Zugriff der US-Muttergesellschaft auf Daten beim Empfänger im EWR ist davon zu unterscheiden:** Er ist ein Fall des **Art. 48 DSGVO** und wird durch keine Garantie nach Art. 46 verhindert. **Die EU-Beschränkung ist enger als sie klingt:** Sie gilt nur bis zur Übergabe an die Telekommunikationsanbieter, und Support-Zugriffe erfolgen auch außerhalb der EU. Merkmal (iii) des Teils B ist für ihn nicht erfüllt (Teil B, Buchstabe d); das gilt für beide Beschränkungen, die nach § 4 Abs. 5a wie die Konfiguration nach § 4 Abs. 6a. **Kurznachrichten aus Arbeitsbereichen des Verantwortlichen** versendet er unter diesen Beschränkungen nicht; technisch gesperrt ist das nur für Arbeitsbereiche, die als öffentliche

Stelle gekennzeichnet sind, im Übrigen stellen wir den Versand bei der Einrichtung der Beschränkung organisatorisch ab.

[6] **Proton.** Ihm fließen Inhalte, Anhänge und Adressdaten der Nachrichten zu — Anmelde-, Einladungs- und Bestätigungsmails, Kündigungs- und Widerrufserklärungen und die über das Kontaktformular eingehenden Anfragen. **Sämtliche anwendungsseitigen Absender** einschließlich beider Marketing-Websites relayen über die Bridge; ein zweiter anwendungsseitiger Versandweg ist nicht vorgesehen. **Der Versand der Rundschreiben läuft nicht über ihn**, sondern außerhalb der Anwendungen. Für die Schweiz besteht ein Angemessenheitsbeschluss (Entscheidung 2000/518/EG vom 26. Juli 2000, fortgeltend nach Art. 45 Abs. 9 DSGVO); Standardvertragsklauseln und ein Transfer-Impact-Assessment sind daneben nicht erforderlich. **Die Brücke betreiben wir selbst in Deutschland**; sie ist kein eigenständiger Sub-Auftragsverarbeiter, sondern der lokale Zugang zu den Postfächern dieses Empfängers. **Postfächer der Kunden:** Bezieht der Verantwortliche Postfächer über uns, liegen auch deren Inhalte, Anhänge und Adressdaten bei der Proton AG (Teil B Buchstabe a). **Vertragsstatus:** Die Proton AG veröffentlicht unter *proton.me/legal/dpa* einen „Data Processing Agreement“ (Stand der Seite: 10.02.2026, abgerufen am 2026-10-14), der nach seinem Wortlaut Teil des Dienstleistungsvertrags nach den Geschäftsbedingungen der Proton AG ist, die Unterauftragsverarbeiter über die Datenschutzerklärung der Proton AG führt und für Übermittlungen außerhalb der Schweiz und des EWR auf Standardvertragsklauseln verweist. **Ob und mit welchem Datum dieser Vertrag für unser Konto gilt, und die Ablage dieses Nachweises, sind noch offen**; deshalb bleibt es bei „in Abschluss“.

[7] **Scaleway.** Ein Teil der Modelle stammt von Herstellern außerhalb der EU (u. a. Qwen, GLM, Llama); verarbeitet wird nur in Frankreich, an die Hersteller wird nichts übermittelt.

[8] **KugelAudio. Die Anschriften weichen voneinander ab:** das Impressum nennt Rosenthaler Str. 36, 10178 Berlin, die Registerdaten die Anschrift Schäfertrift 6, 30657 Hannover. **Eingetragen ist die Gesellschaft beim Amtsgericht Charlottenburg (Berlin), HRB 277989 B**; beide Anschriften liegen in Deutschland, für die Anwendbarkeit von Kapitel V DSGVO kommt es auf die Stadt nicht an. Verarbeitet wird **ausschließlich in der Europäischen Union**. **Zugesichert:** kein KI-Training mit Kundeninhalten ohne gesonderte Einwilligung (§ 12 der Bedingungen). **Die Variante „EU-Only Hosting“ ist nach § 13 Abs. 2 der Anbieterbedingungen gesondert zu bestellen und schriftlich zu bestätigen; beides ist Voraussetzung des Einsatzes** — die Bestellung ist erfolgt; **EU-Hosting durch Bestätigung des Anbieters vom 2026-09-23**, die zur Akte genommen wird. **Ein Endpunktname belegt den Verarbeitungsort nicht:** *api.eu.kugelaudio.com* und der globale Name lösen auf dieselben Adressen auf und teilen ein Zertifikat; zugesichert wird der Verarbeitungsort, nie ein Name. **Ferner offen:** Subprozessorenkette und ein auf diese GmbH lautender Vertrag nach Art. 28 DSGVO — der vorliegende vom 23.01.2026 nennt eine UG in Hannover. **Deshalb die Rolle *AV · ohne Art.-28-Vertrag*** (§ 4 Abs. 4 des Auftragsverarbeitungsvertrags), bis der Vertrag auf die KugelAudio GmbH lautet; sie ist die Beschreibung dieser Lücke und keine Einschränkung der geschuldeten Pflicht. **Für die vom Auftragsverarbeiter selbst betriebenen Agenten ist er zugleich Empfänger in dessen eigener Verantwortlichkeit; die Rollenzelle nennt den strengeren Fall, weil an ihm die Unterrichtung vor der ersten Auswahl hängt.**

[9] **Deepgram.** Die Anbieterfestlegung trifft § 4 Abs. 6 lit. a des Auftragsverarbeitungsvertrags. Ein Einsatz bei den vom Auftragsverarbeiter selbst und den managed betriebenen Agenten setzt eine erneute Transfer-Folgenabschätzung, die Prüfung des Datenschutzbeauftragten und einen nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) tragfähigen Mechanismus voraus; eine Weisung des Verantwortlichen genügt dafür nicht. **Ein Angemessenheitsbeschluss besteht nicht**, und das Transfer-Impact-Assessment **bestätigt die Tragfähigkeit der Standardvertragsklauseln nicht**; welche Folge das hat und was dazu aussteht, nennen die Absätze unter der Tabelle.

[10] **ElevenLabs.** Für **Sprachdaten** von EWR-Nutzern ist die **Eleven Labs Poland sp. z o.o.**, Warschau, eigene Verantwortliche. An keinem Agenten hinterlegt. Modul 3 ist im Vertrag der Sache nach benannt, ohne Modulnummer. **Die DPF-Listung gilt allein für die US-Gesellschaft.**

[11] **Cartesia.** Die Anbieterfestlegung trifft § 4 Abs. 6 lit. b des Auftragsverarbeitungsvertrags. Standardvertragsklauseln **Modul 3 wörtlich**, irisches Recht.

[12] **OpenAI.** Vertragspartnerin für EWR-Kunden ist die **OpenAI Ireland Ltd.**, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43 (CRO 737350). Standardvertragsklauseln **Modul 2 und Modul 3 wörtlich**; **Datenimporteurin ist die US-Gesellschaft**, obwohl die irische Gesellschaft Vertragspartnerin ist.

[13] **Anthropic.** Vertragspartnerin für EWR-Kunden ist die **Anthropic Ireland, Limited**, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29. Standardvertragsklauseln **Modul 2 und 3 wörtlich**, irisches Recht. Die DPF-Registerprüfung am 31.08.2026 ergab, dass **Anthropic PBC dort in keinem Status geführt ist**; ein Angemessenheitsbeschluss besteht somit nicht, die Übermittlung stützt sich allein auf die Standardvertragsklauseln.

[14] **Groq. Vertragspartnerin für den EWR ist die *Groq UK Limited***, 3 Hammersmith Grove, London W6 0ND (Companies House 05087931); Vertreter nach Art. 27 DSGVO: DP-Dock GmbH, Ballindamm 39, Hamburg. **Die Vertragspartnerin sitzt nicht im EWR:** Die Kette läuft über den Angemessenheitsbeschluss für das Vereinigte Königreich, ergänzt um Standardvertragsklauseln **Modul 3 wörtlich**; die EU-Präsenz ist nur ein Vertreter nach Art. 27.

[15] **Perplexity.** Standardvertragsklauseln **Modul 2 und 3** in getrennten Bestimmungen.

[16] **KIE.** Die Bedingungen nennen einen **gemeinsamen Betrieb mit der INNOLEAP AI LLC, deren Rechtsträger und Sitz offen bleiben**. Weitergeleitet wird der Bild-Prompt an **ByteDance Ltd.**, **Alibaba Group** (Qwen, Wan) und **Zhipu AI / Z.ai** — Verarbeitung in der Volksrepublik China —, **Google LLC**, **xAI Corp.**, **Ideogram AI, Inc.** und **OpenAI, L.L.C.** — USA — sowie **Black Forest Labs**, dessen Rechtsträger und Sitz ebenfalls offen sind. Für alle acht sind Rolle, Art.-28-Kette und Kapitel-V-Mechanismus offen; allein für **OpenAI, L.L.C.** bestehen Standardvertragsklauseln aus unserer eigenen Beziehung — **ob sie auch den Weg über KIE decken, ist offen**, denn sie binden OpenAI gegenüber uns, nicht gegenüber KIE. Ohne bestimmten Rechtsträger des Aggregators und ohne abschließend benennbaren Unteranbieterkreis sichern wir weder die Weitergabe der Art.-28-Pflichten noch eine lückenlose Kette nach Kapitel V DSGVO zu (§ 4 Abs. 4 AVV). **Weil für ihn kein Mechanismus nach Kapitel V besteht, bieten wir ihn über die Weisung eines Arbeitsbereichs nicht an; erreichbar ist er nur über die gesonderte Freischaltung je Weg, die keine Grundlage schafft (Festlegung c)** — auch nicht für die Hersteller hinter ihm, für die unsere eigenen Standardvertragsklauseln bestehen: Sie binden den Hersteller gegenüber uns, nicht den Weg über KIE. **Auch im persönlichen Arbeitsbereich schafft keine Erklärung eine Grundlage** — eine Einwilligung nach Art. 49 Abs. 1 Unterabs. 1 lit. a DSGVO ersetzt weder den fehlenden Vertrag nach Art. 28 DSGVO noch trägt sie einen wiederkehrenden Bildpfad (Leitlinien 2/2018 des Europäischen Datenschutzausschusses). § 4 Abs. 4 AVV bleibt geschuldet und ist für ihn nicht erfüllt. Für unsere eigenen und die managed betriebenen Agenten nicht eingesetzt.

[17] **OpenRouter.** Weiterempfänger, Modul der Standardvertragsklauseln und Art.-28-Kette sind unbelegt, ein Vertrag ist nicht zur Akte genommen (§ 4 Abs. 4 AVV). **Einen Mechanismus nach Kapitel V weisen wir deshalb nicht aus** — Standardvertragsklauseln sind nur allgemein behauptet und nicht zur Akte genommen; bis zur vorigen Fassung stand hier *SCC*. Nach Festlegung (c) bieten wir ihn über die Weisung eines Arbeitsbereichs nicht an, bis ein Vertrag mit Modul, Abschlussdatum und Kette vorliegt. **Ob die Abläufe der betreibereigenen Automatisierungsplattform ihn weiter verwenden, ist nicht entschieden**; mit der Entscheidung ziehen wir diese Zeile nach und teilen die Änderung nach § 4 Abs. 2 des Auftragsverarbeitungsvertrags mit.

[18] **Pinecone. Weder ein Vertrag nach Art. 28 DSGVO noch ein Mechanismus nach Kapitel V DSGVO noch ein Transfer-Impact-Assessment liegt für ihn vor** — die Rolle sagt es, und § 4 Abs. 4 des Auftragsverarbeitungsvertrags bleibt für ihn geschuldet. **Er steht damit im Widerspruch zur Festlegung, für den Managed-Betrieb ausschließlich Empfänger in der Europäischen Union einzusetzen.** Der Ablauf ist eingerichtet, ein Fluss derzeit nicht festzustellen; **solange für ihn keine Grundlage besteht, ist der Einsatz zu beenden** und nicht wieder aufzunehmen. Über Ablösung oder Vertragsschluss entscheiden wir; das Ergebnis teilen wir auf Verlangen in Textform mit.

[19] **Linkup.** Übermittelt wird die Suchanfrage. Hosting in der EU, nach Zusage des Anbieters keine dauerhafte Speicherung der Anfrageinhalte (Zero Data Retention).

[20] **Tavily. Die Zugangsdaten sind plattformweit hinterlegt** — die frühere Angabe, es bestünden keine, trifft nicht zu und ist mit dieser Fassung berichtigt. Die Betriebsart **„Janeway Apex“** sah Tavily **vor** Linkup vor. **Für ihn besteht kein Mechanismus nach Kapitel V**, und nach Festlegung (c) bieten wir ihn über die Weisung nicht an; die Plattform weist deshalb jeden Aufruf ab, solange der Weg nicht gesondert freigeschaltet ist, und die Suche übernimmt Linkup (EU). In den EU-Betriebsarten Sentinel und Cortex ist er weder eingestellt noch Rückfallebene. **Unter den Beschränkungen des Teils B steht er nicht zur Verfügung**; die Suche läuft dort auch in der Betriebsart Apex über Linkup. **Für unsere Übermittlungsrichtung ist keine Garantie vereinbart** — die Standardvertragsklauseln des Anbieters gelten gegenüber seinen eigenen Dienstleistern. Der Mechanismus lautet deshalb *OFFEN*, nicht *SCC*; ein Vertrag mit uns, der Modul 3 vereinbart, ist nicht zur Akte genommen.

[21] **WhatsApp.** Es fließen Nachrichteninhalte, Anhänge und Kennungen der Gesprächspartner. Über die weitere Verarbeitung entscheidet der Empfänger eigenständig und ist insoweit eigener Verantwortlicher. **Er sitzt im EWR — Kapitel V ist nicht anwendbar**; die Weitergabe erfolgt auf dem vom Gesprächspartner gewählten Kanal (Art. 6 Abs. 1 lit. b DSGVO).

[22] **Telegram.** Übermittelt werden Nachrichteninhalte, Anhänge und Kennungen der Gesprächspartner, über deren weitere Verarbeitung Telegram eigenständig entscheidet. Die Beschränkung nach Art. 49 Abs. 1 lit. b DSGVO erfasst nur einzelne, vom Gesprächspartner selbst begonnene oder ausdrücklich gewünschte, für dessen Vertrag erforderliche Kommunikation — **regelmäßige oder massenhafte Nutzung und die Spiegelung privater Korrespondenz Dritter sind unzulässig**. **Eine betreibereigene Verbindung weicht von der Beschränkung auf Einzelvorgänge ab und ist zu beenden.**

[23] **CARTO.** Die spanische Zweigniederlassung ist unselbständig und kann nicht Partei eines Vertrags nach Art. 28 DSGVO sein. Die Standortkarte der Agentur-Website lädt erst nach ausdrücklichem Klick auf „Karte laden“; die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) betrifft das Laden, nicht die Übermittlung — diese trägt der Angemessenheitsbeschluss. **Die Lagekarte der Immobilien-Anwendung bezog ihre Kacheln bis zu deren Umstellung ebenfalls von hier; seither kommen sie von der OpenStreetMap Foundation** (nächste Zeile). Der DPF-Registereintrag steht unverändert auf **„Active – Re-certification under Review“** und umfasst nur das Programm EU-U.S. und nur Non-HR-Daten; für unsere Übermittlungen ist Non-HR die einschlägige Kategorie, die Beschränkung also folgenlos. **Die Rezertifizierung war am 24.09.2026 fällig; ein Abruf nach diesem Termin steht aus.**

[24] **OpenStreetMap.** Beide Schnittstellen werden ohne Konto und Nutzungsvereinbarung abgerufen. **Die Ortsauflösung des Wetterwerkzeugs** übermittelt den Ortsnamen aus der Anfrage des Nutzers oder Anrufers — ein Freitextausschnitt — von unseren Servern aus, ohne dessen IP-Adresse. Die Wetterdaten selbst ruft das Werkzeug als öffentliche Dateien beim Deutschen Wetterdienst (Bundesbehörde, Offenbach am Main) ab und übermittelt dorthin nur die Kennung einer Wetterstation, weder Ortsangabe noch Koordinaten; personenbezogene Daten empfängt der Deutsche Wetterdienst damit nicht, und er steht deshalb nicht in dieser Liste. **Die Kacheln lädt der Browser des Besuchers ohne vorherigen Klick**, sobald ein Objekt mit Koordinaten geöffnet wird — auf der öffentlichen Exposé-Seite also auch der Browser eines Interessenten ohne Konto. Die Übermittlung ins Vereinigte Königreich trägt der Angemessenheitsbeschluss. **Für Arbeitsbereiche öffentlicher Stellen stellt die Anwendung diesen Weg nicht bereit** (§ 1 Abs. 8 des Auftragsverarbeitungsvertrags).

[25] **TradingView.** Der Rahmen ist über die Inhaltssicherheitsrichtlinie von *chat.janeway.io* zugelassen und damit ohne weiteres Zutun erreichbar; nach dem Maßstab des § 4 Abs. 1 des Auftragsverarbeitungsvertrags ist er *in Betrieb*. **Ein Mechanismus nach Kapitel V ist für diese Übermittlung nicht vereinbart** und wird deshalb mit *OFFEN* ausgewiesen. Unter den Beschränkungen des Teils B lässt er sich heute nicht je Arbeitsbereich abwählen; er entsteht nur, wenn ein

solcher Baustein geöffnet wird. **Für Arbeitsbereiche öffentlicher Stellen stellt die Anwendung diesen Weg nicht bereit** (§ 1 Abs. 8 des Auftragsverarbeitungsvertrags).

[26] **onOffice.** Ohne hinterlegte Zugangsdaten eines Inhabers fließt nichts; der Status beschreibt den eingerichteten, nicht den benutzten Weg. Sitz und Verarbeitung in Deutschland — Kapitel V ist nicht berührt.

[27] **Push-Zustelldienste.** Die Zustelladresse vergibt der Browser, nicht wir; die Nachricht ist für den Zustelldienst verschlüsselt, und die Freigabe erteilt und entzieht der Nutzer in seinem Browser. **Im Register des EU-U.S. Data Privacy Framework** stehen die Google LLC und die Microsoft Corporation mit *Active* (Abruf 14.10.2026); **die Mozilla Corporation, die den Push-Dienst von Firefox betreibt, und die Apple Inc. sind dort unter den abgefragten Namen nicht geführt**, für sie ist kein Mechanismus ausgewiesen. Standardvertragsklauseln bestehen mit keinem der vier — wir wählen den Dienst nicht und stehen mit ihm in keinem Vertrag. **Für Arbeitsbereiche öffentlicher Stellen stellt die Anwendung diesen Weg nicht bereit** (§ 1 Abs. 8 des Auftragsverarbeitungsvertrags).

Kein Empfänger dieser Liste ist wegen seines Prüfergebnisses gesperrt; wer ohne Mechanismus ist, wird über die Weisung nicht angeboten (Festlegung c). Was fehlt — Mechanismus, Vertrag nach Art. 28 DSGVO, lückenlose Kette —, weist diese Liste aus. **Voreingestellt ist keine Drittlandübermittlung.** Vor der ersten Übermittlung an einen Drittland-Empfänger verlangt die Anwendung die **dokumentierte Weisung** des Arbeitsbereichs nach Art. 28 Abs. 3 Satz 2 lit. a DSGVO — im Firmen-Arbeitsbereich erteilt durch dessen Inhaber oder Administrator, im persönlichen Arbeitsbereich durch die Person selbst; ohne sie wird der Empfänger nicht angesprochen (§ 4 Abs. 5 AVV). **Eine Einwilligung nach Art. 49 DSGVO ist diese Weisung nicht.** Der Inhaber oder Administrator kann Drittland-Empfänger für seinen Arbeitsbereich **sperren**; die Sperre geht einer erteilten Weisung vor. **Daten Unbeteiligter** — Anrufer eines Sprachagenten, Nutzer eines Website-Assistenten — gehen an einen Drittland-Empfänger nur, wenn der Verantwortliche das für den jeweiligen Agenten ausdrücklich bestätigt hat.

Für Behörden in Ausübung hoheitlicher Befugnisse gilt die gesonderte Erklärung nach Art. 49 DSGVO nicht. Art. 49 Abs. 3 DSGVO nimmt sie von den Ausnahmen des Absatzes 1 Unterabs. 1 lit. a bis c aus; die Grenzen und ihre Folge für die Empfängerwahl regelt **§ 1 Abs. 8 des Auftragsverarbeitungsvertrags** („Grenzen des Art. 49 DSGVO bei hoheitlicher Tätigkeit"). **Einer solchen Stelle bieten wir keinen Drittland-Empfänger an, dessen Übermittlung keine Garantie nach Art. 46 DSGVO trägt** — und darüber hinaus **keiner öffentlichen Stelle, gleich ob hoheitlich, einen Drittland-Empfänger des Katalogs** (§ 1 Abs. 8 des Auftragsverarbeitungsvertrags). Ihr stehen für diese Verarbeitungen **zwei** Gruppen nicht zur Verfügung, und beide liest man aus der Spalte „Drittland-Mechanismus": **erstens jede Zeile, die mit *OFFEN* beginnt** — für sie ist kein Mechanismus festgelegt —, **zweitens jede Zeile, für die das Prüfergebnis die Tragfähigkeit der Garantie nicht bestätigt** (*TIA: trägt nicht* oder *TIA: ohne abschließendes Ergebnis*), **auch wenn daneben ein Mechanismus steht**. Für die zweite Gruppe gilt dasselbe wie für die erste; die Begründung steht dort. **Die Spalte ist die Quelle, nicht eine Namensliste daneben** — eine Aufzählung wäre eine Vollständigkeitszusage und bräche bei jeder neuen Zeile still.

Der laufende Betrieb der mit Festlegung (b) gekennzeichneten Drittlandanbieter beruht auf der Auswahl des Verantwortlichen. Für **jede Zeile, deren Zweckspalte die Festlegung (b) trägt**, gilt: Sie bleiben wählbar, die Auswahl ist die dokumentierte Weisung, und vor der ersten Drittlandauswahl wird über Sitz, Verarbeitungsort und Prüfergebnis unterrichtet. Welche Zeilen das sind, sagt die Spalte — nicht eine Namensliste daneben. **Die Entscheidung nach Schritt 4 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses hat die Geschäftsführung am 23.09.2026 getroffen:** Wo wir selbst wählen — die von uns selbst und die managed betriebenen Agenten —, wird ein Empfänger mit *TIA: trägt nicht* nicht eingesetzt. Ausgenommen sind allein die in Festlegung (b) benannten Ausnahmen in unserem eigenen Betrieb — die Betriebsart „Janeway Apex" in unseren eigenen Arbeitsbereichen, für die wir selbst Verantwortliche sind, und die eigenen Demo- und Prüfagenten unserer zweiten Betriebsumgebung. Wählt ein Verantwortlicher Apex für seinen Arbeitsbereich, wählt er und nicht wir; dafür gilt der folgende Satz. Wo der Verantwortliche wählt, ist sie ein **begründeter Fortbetrieb unter Bedingungen**: Voreinstellung ohne Drittlandübermittlung, Weisung nur durch Inhaber oder Administrator, Sperre durch Inhaber oder Administrator,

kein Angebot ohne Mechanismus (Festlegung c), kein Angebot an hoheitlich handelnde Stellen ohne Garantie nach Art. 46 DSGVO und keine Daten Unbeteiligter ohne ausdrückliche Bestätigung je Agent. **Die Entscheidung ist befristet und wird spätestens zum 31.03.2027 neu getroffen**, früher bei jeder Änderung der Rechtslage im Empfängerstaat oder des Mechanismus; verantwortlich ist die Geschäftsführung. Welche Bedingung derzeit nachgewiesen ist, teilen wir auf Verlangen in Textform mit.

> **Ohne Grundlage nach Kapitel V DSGVO.** Für die mit *OFFEN* gekennzeichneten Empfänger ist kein Übermittlungsmechanismus festgelegt. **Welche das sind, sagt die Spalte selbst — nicht eine Aufzählung daneben**, die bei jeder neuen Zeile still bräche. **Ob deshalb auch keine Daten fließen, sagt allein die Spalte Status, und sie sagt es nicht für alle:** Mehrere dieser Zeilen stehen auf *in Betrieb*; dort findet die Übermittlung ohne festgelegten Mechanismus statt. Was im Einzelfall offen ist — ein unbestimmter Rechtsträger, ein fehlender Schritt 3 der Empfehlungen 01/2020, ein Empfänger, dessen Zuordnung noch aussteht —, nennt die jeweilige Zeile. **Nicht hierher gehört die KugelAudio GmbH:** Für sie ist Kapitel V nicht anwendbar (Sitz und Verarbeitung in Deutschland bzw. der Europäischen Union), ihr Mechanismus lautet *EU*; was für sie offen ist, steht in ihrer Zeile.

Restrisiko eines Behördenzugriffs in den Vereinigten Staaten. Empfänger mit Sitz dort unterliegen dem US-Überwachungs- und Herausgaberecht (50 U.S.C. § 1881a, Executive Order 12333, CLOUD Act). Der CLOUD Act erfasst **auch außerhalb der Vereinigten Staaten verarbeitete Daten** sowie Tochtergesellschaften und europäische Rechenzentren, soweit die US-Muttergesellschaft die tatsächliche Verfügungsgewalt hat; ein Serverstandort in der EU schließt ihn nicht aus (EuGH, Urteil vom 16.07.2020, C-311/18 „Schrems II“). Das EU-U.S. Data Privacy Framework (Durchführungsbeschluss vom 10.07.2023) mildert das Risiko, beseitigt es nicht und kann ausgesetzt oder aufgehoben werden. **Es verbleibt daher ein Restrisiko, dass US-Behörden auf die übermittelten Inhalte zugreifen, ohne dass wir hiervon Kenntnis erlangen oder Sie hierüber unterrichten dürfen.** Umgesetzt sind Transportverschlüsselung und Datenminimierung.

Transfer-Impact-Assessment. Ein Assessment je Empfänger nach den Empfehlungen 01/2020 des Europäischen Datenschutzausschusses liegt seit dem 10.08.2026 vor; maßgeblich ist die jeweils geltende Fassung. **Es bestätigt die Tragfähigkeit der Garantie nicht für jeden Empfänger** — diese tragen *TIA: trägt nicht*, darunter sämtliche mit Festlegung (b); die daraus folgende Entscheidung nach Schritt 4 steht im vorletzten Absatz. Für eine Kette, in der wir selbst Auftragsverarbeiter sind, ist **Modul 3** einschlägig; wo wir selbst Verantwortliche sind (Rolle *eigen*), ist es **Modul 2**.

Was von den Verträgen belegt ist, und was nicht — der Stand ist ungleich und wird deshalb einzeln genannt. Für alle nicht als belegt ausgewiesenen Empfänger nennt diese Liste das einschlägige, nicht das nachgewiesene Modul. Abschlussdatum und Anhang II der Standardvertragsklauseln sind für keinen Empfänger abgelegt.

Empfänger	Was belegt ist — und was nicht
OpenAI, Anthropic, Groq, Perplexity, Cartesia	Das vereinbarte **Modul 3** aus dem jeweiligen Vertrag ist **belegt**
ElevenLabs	Modul 3 **der Sache nach benannt, ohne Modulnummer**
Deepgram, CARTO	Modul **nicht ermittelt**
OpenRouter	Standardvertragsklauseln **nur allgemein behauptet**
KIE, Pinecone	**Kein Vertrag nach Art. 28 DSGVO** — beide führen deshalb die Rolle *AV · ohne Art.-28-Vertrag*. Bei KIE ist der Kreis der Weiterempfänger nur benannt, nicht mit Rolle, Vertrag und Mechanismus unterlegt

Proton AG	Vertrag nach Art. 28 DSGVO **in Abschluss** — Vertragstext öffentlich (*proton.me/legal/dpa*), Nachweis der Geltung für unser Konto nicht abgelegt
KugelAudio GmbH	Der abgelegte Vertrag **lautet auf eine andere Gesellschaft** — auch sie führt deshalb die Rolle *AV · ohne Art.-28-Vertrag*
Microsoft	**Product Terms und Data Protection Addendum** noch zur Akte zu nehmen

Den Stand je Empfänger teilen wir auf Verlangen in Textform mit und legen die Garantien nach § 8 des Auftragsverarbeitungsvertrags vor.

Fortlaufende Prüfung der DPF-Listung. Die Listung der US-Empfänger Stripe, Microsoft, Twilio, CARTO, Perplexity und Eleven Labs sowie der Google LLC als Push-Zustelldienst (Fußnote 27) prüfen wir anhand der offiziellen Liste (*dataprivacyframework.gov*) mindestens jährlich sowie **unverzüglich nach jeder bekannten Fälligkeit** der Rezertifizierung. **Nach der Fälligkeit und nicht vor ihr, und das ist Absicht:** Geprüft wird der Status des Registereintrags, nicht der Kalender — vor dem Termin ist an ihm nichts festzustellen. **Bekannte Fälligkeiten:** CartoDB Inc. **24.09.2026**, Perplexity AI, Inc. **08.10.2026**, Eleven Labs Inc. 09.02.2027, Twilio Inc. 20.04.2027, Stripe, LLC 11.05.2027, Microsoft Corporation 31.08.2027. **Alle sechs Listungen sind am 22.09.2026 erneut im Register abgerufen worden und aktiv:** Perplexity, Eleven Labs, Twilio und Stripe mit *Active*, die Microsoft Corporation und CARTO mit *Active – Re-certification under Review*. Die Google LLC steht am 23.09.2026 mit *Active* im Register; ihre Fälligkeit weist der Abruf nicht aus. **Die Microsoft Corporation ist seither rezertifiziert:** Am 14.10.2026 steht sie mit *Active* im Register, nächste Fälligkeit 31.08.2027. **Für die CartoDB Inc. (fällig 24.09.2026) und die Perplexity AI, Inc. (fällig 08.10.2026) steht der Abruf nach der Fälligkeit noch aus**; ihr Status nach diesem Termin ist bis dahin nicht geprüft.

Der genannte Termin ist die Fälligkeit der jährlichen Rezertifizierung (*Next Certification Due Date*), kein Ablaufdatum. Die Listung endet an diesem Tag nicht von selbst; das Register führt für die laufende Prüfung den Status *Active – Re-certification under Review* — CARTO steht seit dem Abruf vom 11.08.2026 in genau diesem Status. Sie entfällt erst, wenn das US-Handelsministerium den Eintrag auf *Inactive Certification – Lapse* setzt. **Geprüft wird deshalb der Status, nicht der Kalender.** Steht ein Eintrag nicht mehr auf *Active*, darf die Übermittlung nur fortgesetzt werden, wenn Standardvertragsklauseln für genau diesen Vertragspartner nachgewiesen und die TIA tragfähig ist.

Vonage ist ausgenommen: Vertragspartner ist die Vonage B.V. mit Sitz in den Niederlanden, für sie ist kein Mechanismus nach Kapitel V erforderlich. **Bei Twilio ist die Listung gleichwohl Teil der Grundlage, und der Grund ist nicht der Konzernzugriff:** Der Vertragspartner sitzt im EWR, die Weiterübermittlung an die Twilio Inc. (USA) ist jedoch ausgewiesen, und für sie tritt der Angemessenheitsbeschluss neben die Standardvertragsklauseln.

No-Training — vertragliche Anforderung, Nachweis offen. Eine Nutzung zu Trainingszwecken muss vertraglich ausgeschlossen sein; die Anbieterbedingung ist je Provider noch zur Akte zu nehmen, bis dahin machen wir keine anbieterbezogene Tatsachenzusage. Für Empfänger ohne Vertragsbeziehung (Rolle *ohne Vertrag*) und für den Aggregator KIE können wir die Einhaltung nicht zusichern.

Empfänger außerhalb der IT-Dienstleistung. Über die Tabelle hinaus geben wir personenbezogene Daten weiter an unser Kreditinstitut zur Abwicklung des Zahlungsverkehrs (Art. 6 Abs. 1 lit. b DSGVO), an unsere Steuerberatung und die Finanzbehörden zur Erfüllung steuer- und handelsrechtlicher Pflichten (Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 257 HGB, § 147 AO) sowie im Einzelfall an Rechtsanwälte, Gerichte und andere Behörden zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 6 Abs. 1 lit. f DSGVO). Für sie sind wir jeweils selbst Verantwortliche (*eigen*), sie sind keine Sub-Auftragsverarbeiter, und eine Übermittlung in Drittländer findet dabei nicht statt.

KI-Verarbeitungsmodi

- **Sentinel und Cortex (Standard):** ausschließlich Modelle von Anbietern mit Sitz in der EU/im EWR — Sentinel auf Mistral AI, Cortex auf Azure OpenAI mit Mistral AI als Rückfallebene; Azure OpenAI verarbeitet mit Ressourcen in Regionen der EU und des EWR, ohne Zusage eines bestimmten Mitgliedstaats, und der Beleg der Bereitstellungsart „Datenzone EU“ steht noch aus (Fußnote 2); Azure AI Speech (Germany West Central) ist die Voreinstellung der Echtzeit-Spracherkennung und für unsere eigenen sowie die managed betriebenen Agenten verbindlich, die SIP-Telefonie läuft über Vonage B.V. oder Twilio Ireland Limited.
- **Apex:** Betriebsart auf Empfängern in den USA (Anthropic, OpenAI, Perplexity, Cartesia; Festlegung b), jedem Arbeitsbereich angeboten, aber nur mit wirksamer Drittland-Weisung wählbar und nirgends Voreinstellung; ohne Weisung ist sie gesperrt.
- **US-Modelle: Für die Empfänger im Katalog ist die Auswahl durch den Verantwortlichen die Weisung** nach Art. 28 Abs. 3 Satz 2 lit. a DSGVO, soweit für den Empfänger ein Mechanismus nach Kapitel V besteht (Festlegung c) — sie ersetzt jedoch nicht die geschuldete Ausweisung: Rechtsträger, Verarbeitungsort, Mechanismus und Prüfergebnis stehen je Empfänger in dieser Liste, einschließlich der Feststellung, dass eines davon fehlt.
- **Sprachmodelle gegen Bildgenerierung:** Im **Sprachmodell**-Katalog sind Anbieter mit Verarbeitung in Drittländern ohne Angemessenheitsbeschluss und ohne tragfähige Garantien nicht hinterlegt, insbesondere solche mit Verarbeitung in der Volksrepublik China (z. B. DeepSeek). **Für die Bildgenerierung gilt dasselbe:** Die Modelle von ByteDance (Seedream), Alibaba Group (Qwen, Wan) und Zhipu AI / Z.ai (Z-Image), drei Herstellern mit Verarbeitung in der Volksrepublik China, führen wir nicht mehr im Katalog; der Aggregator KIE selbst wird über die Weisung nicht angeboten (KIE-Zeile).

Teil B — die Empfänger, die bei beiden Beschränkungen bleiben (§ 4 Abs. 5a und Abs. 6a)

Wofür Teil B gilt — eine Liste, zwei Beschränkungen. Diese Liste gilt in zwei Fällen, und sie sind nicht dasselbe: **(a)** Der Verantwortliche verlangt in Textform die **Beschränkung auf Teil B** (§ 4 Abs. 5a des Auftragsverarbeitungsvertrags); dann setzen wir für seine Arbeitsbereiche ausschließlich die Empfänger der nachstehenden Tabelle und die darunter abschließend benannten Wege ein, **und der Sprachkanal bleibt nutzbar** — die Wege b) bis d) sind gerade die, die ihn tragen. **(b)** Er verlangt zusätzlich die **Konfiguration „Verarbeitung im EWR“** (§ 4 Abs. 6a); sie geht darüber hinaus und **schließt den Sprachkanal aus**. Welches von beidem gilt, kreuzt er in **Anlage 5 Ziffer 2** an. **Teil B ist eine Teilmenge des Teils A und aus ihm abgeleitet**; für Rolle, Status, Mechanismus und die offenen Punkte je Empfänger bleibt dort dessen Zeile maßgeblich.

Das Kriterium ist kumulativ. In der nachstehenden Tabelle steht ein Empfänger nur, wenn Teil A für ihn zugleich ausweist: **(i)** Verarbeitungsort ausschließlich in der Europäischen Union oder im Europäischen Wirtschaftsraum, **(ii)** Rechtsträger mit Sitz in der Union oder im EWR und **(iii)** keine Verfügungsgewalt eines Mutter- oder Konzernunternehmens aus einem Drittland über die Verarbeitung (Art. 48 DSGVO). **Wer eines der drei nicht erfüllt, steht nicht in der Tabelle — auch dann nicht, wenn für ihn ein Mechanismus nach Kapitel V besteht.** Wo wir den Weg gleichwohl selbst bestimmen und er sich nicht abwählen lässt, steht er darunter, namentlich und mit dem Merkmal, das ihm fehlt.

Was das Kriterium nicht ist. Es lautet **nicht** „kein Unternehmen mit Muttergesellschaft in einem Drittstaat“. Ob eine Konzernstelle in einem Drittland auf Daten zugreifen kann, die bei einem Empfänger im EWR liegen, ist ein **eigener Tatbestand nach Art. 48 DSGVO** und wird durch keine Übermittlungsgarantie beantwortet; wo diese Frage sich stellt, benennen wir sie in der Zeile, statt sie in den Mechanismus zu ziehen. **Eine Zusicherung, dass für die Empfänger des Teils B ein solcher Zugriff ausgeschlossen sei, geben wir nicht.** Die serverseitige Schranke entscheidet über den Verarbeitungsort; Konzernverhältnisse kennt sie nicht.

Empfänger (Rechtsträger, Sitz)	Funktion unter diesen Beschränkungen	Grundlage der Aufnahme und offener Punkt
Hetzner Online GmbH, Gunzenhausen, Deutschland	Hosting sämtlicher Anwendungen, Datenbank, Objektspeicher, Anmeldung; darauf betreiben wir den Datenbank- und Anmelde-Stack, den Echtzeit-Audio-Server und das interne KI-Gateway selbst	Sitz und Verarbeitung Deutschland; kein Drittlandbezug. Die selbst betriebenen Bestandteile sind keine eigenständigen Empfänger
Mistral AI SAS, Paris, Frankreich	KI-Sprachmodelle des EU-Standardbetriebs: **Voreinstellung der Betriebsart Sentinel**, Rückfallebene der Betriebsart Cortex und, wo so eingerichtet, gewähltes Gesprächsmodell des Sprachkanals; **für öffentliche Stellen tritt Mistral an die Stelle von Azure OpenAI**, das Teil B nicht führt — die Umstellung nimmt der Auftragsverarbeiter bei der Einrichtung des Arbeitsbereichs vor (§ 4 Abs. 5a AVV); Text-Einbettungen	Sitz und Verarbeitung Frankreich
Scaleway SAS, Paris, Frankreich	KI-Sprachmodelle, Text-Einbettungen und Sprache-zu-Text **außerhalb** des Echtzeit-Sprachpfads	Sitz und Verarbeitung Frankreich; an die Modellhersteller außerhalb der EU wird nichts übermittelt
Linkup Technologies SAS, Fresnes, Frankreich	Web-Suche — Standard-Backend der Recherche	Sitz und Verarbeitung Frankreich
SearXNG, von uns selbst auf Hetzner betrieben, Deutschland	Web-Suche als Auffangnetz hinter Linkup	von uns selbst in Deutschland betrieben; kein eigenständiger Empfänger

Vier Wege, die wir selbst bestimmen — abschließend, mit Rechtsträger, Sitz und Grundlage (§ 4 Abs. 6a des Auftragsverarbeitungsvertrags verlangt genau diese Angaben). Sie stehen nicht in der Tabelle, und keiner von ihnen lässt sich durch eine der beiden Beschränkungen abwählen. **Wer einen von ihnen nicht in Kauf nimmt, kann die betreffende Leistung nicht beziehen.**

Einer gilt unabhängig vom gewählten Leistungsumfang — für die Postfächer, sobald der Verantwortliche sie über uns bezieht:

a) **System- und Betreiberpost sowie die über uns bezogenen Postfächer** — **Proton AG**, Route de la Galaise 32, 1228 Plan-les-Ouates, Genf, **Schweiz**: Anmelde-, Einladungs- und Bestätigungsmails, Kündigungs- und Widerrufserklärungen und die Anfragen aus dem Kontaktformular; **bezieht der Verantwortliche Postfächer über uns, werden auch sie dort betrieben** — Inhalte, Anhänge und Adressdaten der Nachrichten liegen dann bei der Proton AG und werden über unsere selbst betriebene Brücke in Deutschland angebunden. **Grundlage: Angemessenheitsbeschluss für die Schweiz** (Art. 45 DSGVO). **Ein zweiter anwendungsseitiger Versandweg besteht nicht. Vertragsstatus: Ein Vertrag nach Art. 28 DSGVO mit der Proton AG ist in Abschluss und liegt noch nicht vor (Teil A)**; bis zu seiner Vorlage ist die Vertragskette für beide Teile dieses Weges nicht belegt. Für öffentliche Stellen nehmen wir den Postfachbetrieb mit personenbezogenen Echtdaten erst auf, wenn der Nachweis nach Teil A vorliegt und wir ihn der öffentlichen Stelle vorgelegt haben. **Die Schriftart dieser Nachrichten kommt aus eigener Infrastruktur** und begründet keinen weiteren Empfänger.

Drei fallen nur an, wenn der Sprachkanal gewählt ist. Für die Echtzeit-Spracherkennung erfüllt kein Anbieter alle Merkmale des Teils B; welche der beiden Beschränkungen den Sprachkanal deshalb ausschließt und welche ihn zulässt,

steht in **Anlage 5 Ziffer 2** des Auftragsverarbeitungsvertrags — an der Stelle, an der der Verantwortliche wählt. Die Rechtsfolge regelt § 4 Abs. 6a und wird hier nicht wiederholt.

b) **Echtzeit-Spracherkennung** — **Microsoft Ireland Operations Limited**, Dublin, **Irland**, Verarbeitung in Deutschland (Region Germany West Central). **Grundlage: Empfänger im EWR**, Kapitel V auf die Übermittlung an ihn nicht anwendbar, ergänzend Standardvertragsklauseln. **Kein Anbieter der Echtzeit-Spracherkennung erfüllt alle drei Merkmale des Teils B** — der einzige andere wählbare verarbeitet in den Vereinigten Staaten. **Der gesamte Sprach- und Chatpfad verarbeitet im EWR; der Drittlandbezug der Spracherkennung liegt allein in der Verfügungsgewalt der US-Konzernmutter** (CLOUD Act). Das ist ein Fall des **Art. 48 DSGVO**, gesondert bewertet in unserem Transfer-Impact-Assessment (Ziff. 5.5). **Schaltet der Verantwortliche Microsoft Azure ab, endet der Telefon-Agent mit einem Hinweis, solange kein vereinbarter Rückfall für die Echtzeit-Spracherkennung besteht** (§ 4 Abs. 5b des Auftragsverarbeitungsvertrags). **Die übrigen Microsoft-Wege des Teils A gehören nicht hierher:** Azure OpenAI setzen wir als Gesprächsmodell der Betriebsart Cortex und der managed betriebenen Agenten ein; es erfüllt Merkmal (iii) nicht, und unter beiden Beschränkungen tritt deshalb Mistral AI (Tabelle) an seine Stelle. Microsoft Graph und der Postfachabruf über IMAP richtet der Nutzer selbst ein; sie entstehen ohne Zutun des Verantwortlichen nicht. Unsere Rundschreiben über Microsoft Exchange Online versenden wir als eigene Verantwortliche; sie sind kein Weg der Auftragsverarbeitung.

c) **Sprachsynthese** — **KugelAudio GmbH**, Sitz **Deutschland**, Amtsgericht Charlottenburg HRB 277989 B. **Grundlage: Empfänger im EWR mit Verarbeitung in der Europäischen Union**, Kapitel V nicht anwendbar. Geschuldet ist die Variante „EU-Only Hosting“; EU-Hosting durch Bestätigung des Anbieters vom 2026-09-23. **Merkmal (i) ist nicht ausgewiesen:** Die Subprozessorenkette ist nicht erhoben. Offen ist außerdem ein auf diese Gesellschaft lautender Vertrag nach Art. 28 DSGVO (Teil A). **Alternativ** erbringt die Sprachsynthese die **Microsoft Ireland Operations Limited** über Azure AI Speech in der Region Germany West Central — mit derselben Grundlage und demselben Merkmal, das ihr fehlt, wie unter Buchstabe b.

d) **Zuführung eingehender Anrufe (SIP)** — **Vonage B.V.**, Radarweg 29 A, 1043 NX Amsterdam, **Niederlande** (KVK 34223740). **Grundlage: Empfänger im EWR**, Kapitel V auf die Übermittlung an ihn nicht anwendbar. **Merkmal (i) ist nicht ausgewiesen:** Ob innerhalb der Unternehmensgruppe (Ericsson AB) in ein Drittland weiterübermittelt wird, ist Gegenstand einer laufenden Erhebung, und im Register des EU-U.S. Data Privacy Framework ist mit der **Vonage Holdings Corp.**, Holmdel, New Jersey, eine Gesellschaft dieser Gruppe in den Vereinigten Staaten geführt. **Deshalb steht Vonage nicht in der Tabelle.** Ergibt die Erhebung eine Weiterübermittlung, ist für sie ein Mechanismus nach Kapitel V auszuweisen. **Die Twilio Ireland Limited steht hier nicht, obwohl sie Anrufe ebenfalls zuführt:** Für sie ist die Weiterübermittlung an die Twilio Inc. (USA) ausgewiesen — **Merkmal (i) ist damit nicht erfüllt**, der Verarbeitungsort liegt nicht ausschließlich in der Union oder im EWR; der Konzernzugriff nach Merkmal (iii) tritt hinzu. **Dasselbe Merkmal trägt den Ausschluss der Vonage B.V.**, dort mangels Erhebung als „nicht ausgewiesen“ statt als „nicht erfüllt“. Unter beiden Beschränkungen erfolgt die Zuführung deshalb **ausschließlich über die Vonage B.V.** (§ 4 Abs. 5a des Auftragsverarbeitungsvertrags); liegt die Rufnummer eines Arbeitsbereichs bei Twilio, wird sie vor der Einrichtung umgestellt, und ist das nicht möglich, wird der Sprachkanal für diesen Arbeitsbereich nicht in Betrieb genommen. **Die Beschränkung „insoweit nicht einzurichten“ ist kein zulässiger Weg** — auch nicht für Arbeitsbereiche, in denen im Sprachkanal regelmäßig besondere Kategorien nach Art. 9 DSGVO anfallen (Ziff. 4 der Präambel des Auftragsverarbeitungsvertrags).

Was diese Beschränkungen leisten — und was sie nicht leisten. Für jeden Anbieter, den der Anbieterkatalog als Drittland-Anbieter führt, verweigert die Anwendung die Herausgabe der Zugangsdaten und damit die Verarbeitung, solange der Arbeitsbereich keine Drittland-Weisung führt oder Drittland-Empfänger gesperrt hat; das gilt auch auf dem Sprachpfad, und **ein nicht eingestufter Anbieter gilt dabei als Drittland-Anbieter-**. **Das ist der Auslieferungszustand und keine gesondert zu bestellende Leistung.** Außerhalb dieses Katalogs liegen allein die Buchstaben a bis d und die Wege, die mit der jeweiligen Anwendung, Funktion oder

Schnittstelle abgewählt werden — Kartenkacheln und Geocoding der Immobilien-Anwendung, Ortsauflösung des Wetterwerkzeugs der Agenten (OpenStreetMap Foundation, Vereinigtes Königreich), die Messenger-Anbindungen und deren Benachrichtigungszustellung, die Immobilien-Anbindung an onOffice, der Kurs-Chart des AI Chat und die vom Nutzer selbst eingerichteten Microsoft-Schnittstellen; sie entstehen ohne die entsprechende Anwendung, Funktion oder Verbindung nicht. **Der Kurs-Chart lässt sich heute nicht je Arbeitsbereich abschalten**; er entsteht erst, wenn ein Nutzer einen solchen Baustein öffnet. **Für Arbeitsbereiche öffentlicher Stellen stellt die Anwendung die Wege dieser Aufzählung, die ein Drittland berühren, nicht bereit** — Kurs-Chart, Kartenkacheln und Ortsauflösung über OpenStreetMap, Benachrichtigungszustellung des Messengers, Telegram-Anbindung und die Microsoft-Schnittstellen (§ 1 Abs. 8 des Auftragsverarbeitungsvertrags); außerhalb der EU und des EWR bleibt dort allein Buchstabe a. **Nicht erfasst sind Ziele, die der Verantwortliche selbst bestimmt** — etwa die Adresse eines Webhooks oder einer HTTP-Anfrage in einem Ablauf.

Zwei Grenzen benennen wir ausdrücklich, weil ohne sie die Zusage weiter reichte als der Mechanismus:

1. **Die Schranke entscheidet über den Verarbeitungsort, nicht über Konzernverhältnisse.** Ein Empfänger mit Sitz und Verarbeitung im EWR passiert sie auch dann, wenn eine Konzernstelle in einem Drittland auf ihn zugreifen könnte. Diese Frage beantworten die Buchstaben b und d, nicht die Beschränkung.
2. **Die Weisung wirkt für den gesamten Arbeitsbereich.** Im Firmen-Arbeitsbereich erteilen sie nur Inhaber oder Administrator; wer den Betrieb ohne Drittlandempfänger dauerhaft sicherstellen will, **sperrt** Drittland-Empfänger für seinen Arbeitsbereich — die Sperre geht einer erteilten Weisung vor. **Auf Verlangen weisen wir die für einen Arbeitsbereich erteilten Weisungen und Sperren in Textform nach und setzen einen Widerruf um.**

Fassung dieser Liste: 14. Oktober 2026, Partial-Fassung 2.31.6, Erhebungsstichtag 2026-10-14. Maßgeblich für Stand und Fassung des Dokuments, in das sie eingezogen ist, ist dessen Vorspann; Änderungen dieser Liste teilen wir unseren Auftraggebern nach § 4 Abs. 2 des Auftragsverarbeitungsvertrags mit. Die Änderungen der früheren Fassungen sind gesondert dokumentiert und werden auf Verlangen vorgelegt.

Anlage 4: Löschkonzept

Wahlrecht, Fristen, Formate, Transportweg, Umfang der Rückgabe, Löschverfahren und Inhalt des Protokolls regelt § 7 dieses AVV abschließend.

Anlage 5: Vereinbarter Leistungsumfang

Diese Anlage bestimmt, welche Kanäle Gegenstand der Verarbeitung sind und welche der beiden Beschränkungen nach § 4 Abs. 5a und Abs. 6a gelten. Sie wird beim Abschluss ausgefüllt; bleibt sie leer, gilt der im Hauptvertrag beauftragte Umfang.

1. Kanäle — Zutreffendes ankreuzen; beide Felder sind zulässig.

	Kanal	Umfasst
[ ]	**Schriftliche Kanäle**	Chat-Widget, Postfach und E-Mail, Wissenssuche, Chat-Assistenten und Workflows ohne Sprachanteil
[ ]	**Sprachkanäle**	KI-Telefonie und Web-Sprach-Widget; welche Wege sie auslösen, benennt Teil B der Anlage 3

Was die Wahl entscheidet: Welche der selbst bestimmten Wege **nur** bei angekreuzten Sprachkanälen anfallen, benennt **Teil B der Anlage 3** abschließend; sie sind der Grund, warum Sprachkanal und die Konfiguration nach **Ziffer 2 Buchstabe b** einander ausschließen (§ 4 Abs. 6a). Wird nur der schriftliche Umfang gewählt, entfallen sie; die vom Leistungsumfang unabhängigen Wege des Teils B bleiben unberührt. **Mit der Beschränkung nach Ziffer 2 Buchstabe a bleibt der Sprachkanal dagegen nutzbar** — sie erfasst die in Teil B abschließend benannten Wege nicht.

2. Beschränkung der Empfänger — zwei getrennte Festlegungen. Buchstabe a ist die engere Empfängerwahl und lässt den Sprachkanal zu; Buchstabe b tritt hinzu und schließt ihn aus. Buchstabe b setzt Buchstabe a voraus.

Diese Anlage ist der Ort dieser Festlegung. Ein gleichlautendes Feld an anderer Stelle des Vertragswerks — insbesondere im Leistungs- und Anbieterschein — gibt sie wieder und ersetzt sie nicht; weichen beide voneinander ab, gilt diese Anlage (§ 10 Abs. 1).

a)	[ ]	**Beschränkung auf Teil B der Anlage 3** (§ 4 Abs. 5a) — für sämtliche Arbeitsbereiche des Verantwortlichen werden ausschließlich die dort geführten Empfänger eingesetzt. **Der Sprachkanal bleibt nutzbar:** Die in Teil B abschließend benannten Wege — darunter Spracherkennung, Sprachsynthese und die Zuführung eingehender Anrufe — sind von dieser Beschränkung nicht erfasst und bleiben es auch nicht
b)	[ ]	**zusätzlich die Konfiguration „Verarbeitung im EWR“** (§ 4 Abs. 6a) — es findet keine Übermittlung an einen Empfänger außerhalb des EWR statt, für die dieser Vertrag eine Wahl vorsieht. **Sie schließt den Sprachkanal aus**

Warum Buchstabe b den Sprachkanal ausschließt und Buchstabe a nicht: Für die Echtzeit-Spracherkennung steht kein Anbieter zur Verfügung, der alle Merkmale des Teils B erfüllt (§ 4 Abs. 6a). Buchstabe a nimmt die selbst bestimmten Wege ausdrücklich aus und lässt den Kanal deshalb unberührt; Buchstabe b tut das nicht. **Wird Buchstabe b angekreuzt, bleibt der Sprachkanal unter Ziffer 1 unangekreuzt**; die schriftlichen Kanäle sind in beiden Fällen uneingeschränkt nutzbar. Wird der Sprachkanal später hinzugewählt, endet die Konfiguration nach Buchstabe b mit seiner Inbetriebnahme (§ 4 Abs. 6a); Buchstabe a bleibt bestehen.

Für öffentliche Stellen ist Buchstabe a die Voreinstellung (§ 4 Abs. 5a) — **Buchstabe b ist es nicht.** Eine öffentliche Stelle mit Bürgertelefon wählt daher Buchstabe a, nicht Buchstabe b. Wird Buchstabe a abgewählt, ist das eine Weisung nach § 1 Abs. 1; auf ihre Rechtsfolgen weist der Auftragsverarbeiter nach § 1 Abs. 4 hin. **Bei öffentlichen Stellen ist das Kreuz in dieser Anlage zugleich die Weisung in der Form, in der dieser Vertrag geschlossen wurde** (§ 4 Abs. 5a); einer weiteren Erklärung bedarf es nicht.

Was die Abwahl NICHT öffnet: Für Anruferinnen und Anrufer, Gesprächspartner und Nutzer der Widgets genügt auch dann die Drittland-Weisung des Arbeitsbereichs nicht; ein Agent spricht für sie einen Drittland-Empfänger nur auf die gesonderte Weisung je Agent an, und Empfänger **ohne** Mechanismus nach Kapitel V DSGVO (Art. 45, 46 oder 47 DSGVO) bleiben ausgeschlossen (§ 4 Abs. 5, zweiter Unterabsatz). **Ein Empfänger mit Mechanismus bleibt wählbar** — einer öffentlichen Stelle nicht (§ 1 Abs. 8 Unterabs. 2) —, und **über die Spracherkennung eigener Agenten des Verantwortlichen entscheidet dieser** (§ 4 Abs. 6 lit. a). Für Verarbeitungen in Ausübung hoheitlicher Befugnisse gilt zusätzlich § 1 Abs. 8; die übrigen Anbieterfestlegungen des § 4 Abs. 6 bleiben unberührt.

3. Ergänzende Vereinbarungen zum Leistungsumfang

Kontaktstellen

	Auftragsverarbeiter	Verantwortlicher
Kontaktstelle für Weisungen (§ 1) und datenschutzrechtliche Anfragen	legal@janeway.io	_____
Meldestelle für Verletzungen des Schutzes personenbezogener Daten (§ 6 Abs. 2)	legal@janeway.io	_____
Rufnummer für Rückfragen zu einer Meldung (§ 6 Abs. 2) — sie ist **kein** Meldeweg; die Meldung geht per E-Mail an die vorstehende Meldestelle	+49 176 41 41 61 21	_____
Datenschutzbeauftragter — bei öffentlichen Stellen der behördliche Datenschutzbeauftragte (Art. 37 Abs. 1 lit. a DSGVO)	siehe Abschnitt „Parteien“	_____
Weisungsberechtigte Personen (§ 1 Abs. 2)	—	_____
Zuständige Aufsichtsbehörde (§ 6 Abs. 5)	—	_____

Abschluss

Für die Nutzung der Janeway Suite kommt dieser AVV in der bei Vertragsschluss abrufbaren Fassung **mit der Zustimmung zu den Allgemeinen Geschäftsbedingungen nach deren § 9 Abs. 3 i. V. m. § 1 Abs. 4 zustande** — mit der Registrierung des Arbeitsbereichs und unabhängig von einem kostenpflichtigen Abonnement. Die nachstehende Unterzeichnung ist dafür nicht erforderlich; sie steht dem Verantwortlichen frei, wenn er die Angaben des Abschnitts „Parteien“ verbindlich festlegen will.

Öffentliche Stellen. Ist der Verantwortliche eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, kommt dieser AVV **nicht** durch Zustimmung in der Anwendung zustande. Er wird in diesem Fall mit ausgefülltem Abschnitt „Parteien“, ausgefüllter Tabelle „Kontaktstellen“, ausgefüllter **Anlage 5**, einem gezeichneten **Leistungs- und Anbieterschein** — in dem die eingesetzten Empfänger je Leistung angekreuzt sind — und der Erklärung der nach dem für den Verantwortlichen geltenden Recht vertretungsberechtigten Person geschlossen; die Textform des Art. 28 Abs. 9 DSGVO genügt, soweit das für ihn geltende Recht keine strengere Form verlangt. **Verpflichtungserklärungen einer Gemeinde bedürfen nach den Gemeindeordnungen der Länder regelmäßig der Schriftform und der Unterzeichnung durch den Hauptverwaltungsbeamten oder seinen Vertreter; welche Vorschrift für ihn gilt, benennt der Verantwortliche.** Der Auftragsverarbeiter stellt dafür ein vorbereitetes, zeichenbares Exemplar bereit, hält den geschlossenen Vertragstext für die Dauer des Hauptvertrags vor und stellt ihn auf Verlangen in Textform zur Verfügung. **Bis zum Abschluss darf der Verantwortliche den Arbeitsbereich nur zur Erprobung ohne personenbezogene Echtdaten nutzen.**

Zum Nachweis: Der Auftragsverarbeiter protokolliert das Zustandekommen dieses AVV mit zustimmendem Nutzerkonto und Zeitpunkt, **die Fassungsbezeichnung seit dem 2026-08-26**; ebenso für die Allgemeinen Geschäftsbedingungen und die Bedingungen der einzelnen Anwendungen. **Zustimmungen vor dem 2026-08-26 führen die Fassung als unbekannt, und das ist nicht nachholbar:** Sie belegen Konto und Zeitpunkt, nicht den zugestimmten Text. Eine nachträglich hergeleitete Zeile wird zusätzlich als solche gekennzeichnet und ist **kein Nachweis des Zustandekommens.** Den Nachweis legt er nach § 8 Abs. 1 vor. Eine automatische Übernahme der

„Parteien“-Angaben aus den Kontodaten und ein dauerhafter Abruf des Vertragstexts über die Anwendung bestehen nicht; den geltenden Text stellt er auf Verlangen in Textform zur Verfügung (Art. 28 Abs. 9 DSGVO).

Im Übrigen — insbesondere bei Rahmenverträgen und Leistungsscheinen — wird dieser AVV mit der Unterzeichnung beider Parteien wirksam, nach Art. 28 Abs. 9 DSGVO auch elektronisch. Er gilt für die Laufzeit des Hauptvertrags; § 7 bleibt darüber hinaus anwendbar.

Auftragsverarbeiter	**Verantwortlicher**
Ort, Datum: _____	Ort, Datum: _____
_____	_____
Janeway.io UG (haftungsbeschränkt), vertreten durch Lukas Pritzkow	Name, **Amtsbezeichnung** oder Funktion
	_____
	Name, **Amtsbezeichnung** oder Funktion — *zweite Unterschrift, soweit das Recht des Auftraggebers sie verlangt*
	Rechtsgrundlage der Vertretungsberechtigung: _____ — *je Unterzeichnendem gesondert; bei zwei Unterschriften beide angeben*

Vertrags-/Kundennummer: _____

*Bei öffentlichen Stellen richten sich **Form und Vertretung** der Erklärung, durch die sich der Auftraggeber verpflichtet, nach dem für ihn geltenden Recht — regelmäßig der Gemeinde-, Landkreis- oder Verwaltungsordnung seines Landes. Diese verlangen vielfach die **Schriftform** und die **handschriftliche** Unterzeichnung unter Beifügung der **Amtsbezeichnung**, lassen daneben eine **dauerhaft überprüfbare qualifizierte elektronische Signatur** zu und sehen im Vertretungsfall teils **zwei** vertretungsberechtigte Bedienstete vor. **Welche Vorschrift gilt und wie viele Unterschriften sie verlangt, benennt der Auftraggeber**; der Auftragnehmer prüft es nicht. Die zweite Zeile bleibt frei, wenn eine Unterschrift genügt. **Verlangt jenes Recht einen Vertretungsvermerk** (etwa „in Vertretung“, „im Auftrag“), setzt der Unterzeichnende ihn neben seine Amtsbezeichnung.*

*Statt handschriftlich kann der Auftraggeber **qualifiziert elektronisch signieren**: Er sendet das signierte Exemplar an legal@janeway.io; der Auftragnehmer prüft die Signatur, bestätigt den Eingang in Textform und bewahrt das Exemplar für die Dauer der gesetzlichen Aufbewahrungsfristen auf. **Ob die Signatur „dauerhaft überprüfbar“ im Sinne der für den Auftraggeber geltenden Vorschrift ist — also beweiswerterhaltend aufbewahrt wird —, richtet sich nach dessen Recht und liegt bei ihm; der Auftragnehmer schuldet die Aufbewahrung, nicht den Beweiswerterhalt.** Der Auftragnehmer zeichnet auf demselben Weg gegen.*

Die Änderungsgeschichte wird in der Versionsverwaltung geführt und auf Anforderung vorgelegt. Die geltende Fassung steht im Kopf; welche Fassung der Anlage 3 sie trägt, weist diese selbst aus (§ 4 Abs. 2, Anlage 3); Anlage 2 gilt mit der Fassung dieses Vertrags.