Hinoa - Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO · Stand: 17. August 2026

zwischen

HiNoa UG (haftungsbeschränkt)

Knaackstr. 84, 10435 Berlin

nachfolgend der „Auftragsverarbeiter" / „Hinoa"

und dem im jeweiligen Order Form benannten Auftraggeber.

1. Art, Zweck, Gegenstand und Rechtsgrundlage der Datenverarbeitung

DSGVO. Diese Auftragsverarbeitungs-Vereinbarung legt die Bedingungen für die Verarbeitung personenbezogener Daten durch Hinoa unter Billigung des Auftraggebers in Übereinstimmung mit der Datenschutzgrundverordnung (DSGVO) fest. Hinoa handelt als Auftragsverarbeiter im Sinne der DSGVO.

Art, Zweck und Gegenstand. Hinoa verarbeitet personenbezogene Daten auf dokumentierte Weisung des Auftraggebers, um die Bereitstellung und den Betrieb der von Hinoa angebotenen Software-, Cloud- oder KI-gestützten Dienste zu ermöglichen.

Dazu zählen insbesondere – jedoch nicht abschließend – Dienste zur Kommunikation, Prozessautomatisierung und Datenverarbeitung im Immobilienbereich:

- KI-gestützte Telefon- und Sprachassistenten (Inbound, Cowork und Outbound)
- Kalender- und E-Mail-Management
- CRM-Systeme
- automatisierte Dokumentenverarbeitung
- Analyse- und Reporting-Module

Die personenbezogenen Daten werden ausschließlich verarbeitet, soweit dies für die Nutzung der Hinoa-Dienste erforderlich ist. Der Auftraggeber stellt die dafür notwendigen Daten in geeigneter elektronischer Form zur Verfügung.

Soweit zwischen den Parteien ein zusätzlicher Vertrag (insbesondere Order Form mit MSA) besteht, ergänzt dieser AVV die dort vereinbarten Leistungen. Besteht kein weiterer Vertrag, gelten die in diesem Dokument beschriebenen Zwecke als Grundlage der Datenverarbeitung im Sinne von Art. 28 Abs. 3 DSGVO.

2. Betroffene personenbezogene Daten und Kategorie betroffener Personen

Im Rahmen der vereinbarten Leistungen können insbesondere die folgenden Daten verarbeitet werden:

- Stammdaten (z.B. Name, Kontaktdaten, Rufnummer)
- Audio-Sprach-Daten und damit verbundene sprachlich übermittelte personenbezogene Daten (ausschließlich flüchtige Verarbeitung in Echtzeit, keine Speicherung von Audio)
- Kommunikations- und Inhaltsdaten (z.B. Nachrichten, Gesprächstranskripte, Gesprächszusammenfassungen)

- Nutzungs- und Metadaten (z.B. Zeitpunkt, Dauer, Endgrund eines Gesprächs)
- KI-generierte Inhalte sowie Protokolle der vom KI-Assistenten ausgeführten Aktionen (z.B. CRM-Abfragen, Terminbuchungen, E-Mail-Versand) einschließlich der dabei verarbeiteten Inhalte
- Daten im Zusammenhang mit der Servicequalität
- Vom Auftraggeber für ausgehende Kommunikation bereitgestellte Kontakt- und Adressbestände, einschließlich Angaben zur jeweiligen Rechtsgrundlage der Ansprache

Der Auftraggeber nimmt zur Kenntnis, dass Hinoa keinen Einfluss auf die im Rahmen der Leistungserbringung verarbeiteten Kategorien personenbezogener Daten hat. Dies betrifft insbesondere die mögliche Übermittlung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO). Der Auftraggeber stellt sicher, dass besondere Kategorien personenbezogener Daten nicht übermittelt werden, soweit dies in seinem Einflussbereich liegt, und richtet seine Konfiguration entsprechend aus. Teilt eine betroffene Person solche Daten unaufgefordert im Gespräch mit, verarbeitet Hinoa diese ausschließlich im Rahmen der Weisungen des Auftraggebers.

Von der Verarbeitung sind grundsätzlich die folgenden Kategorien betroffener Personen erfasst:

- Bestehende und potenzielle Kunden des Auftraggebers (insbesondere Eigentümer, Verkäufer, Kauf- und Mietinteressenten, Mieter)

Ferner: Mitarbeiter und Beauftragte des Auftraggebers, deren Kommunikations- und Kalenderdaten im Rahmen von Noa Cowork verarbeitet werden; Geschäftspartner und Dienstleister des Auftraggebers (z. B. Hausverwaltungen, Notare, Gutachter, Handwerksbetriebe); sonstige Personen, die den Auftraggeber telefonisch oder per Nachricht kontaktieren; sowie Personen, die der Auftraggeber im Rahmen ausgehender Kommunikation kontaktiert und deren Kontaktdaten er Hinoa hierfür bereitstellt. Für das Vorliegen einer Rechtsgrundlage der Ansprache dieser Personen ist der Auftraggeber allein verantwortlich (Ziffer 7; § 5 MSA).

Der Auftraggeber informiert Hinoa über alle erforderlichen Änderungen an der vorstehenden Liste.

3. Bedingungen der Datenverarbeitung

Hinoa verpflichtet sich, während der gesamten Leistungserbringung sämtliche Vorgaben der DSGVO einzuhalten.

Hinoa verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Weisungsbefugt ist der im Order Form benannte Ansprechpartner des Auftraggebers sowie jede von ihm hierzu benannte Person. Hinoa ist nicht verpflichtet, Weisungen des Auftraggebers rechtlich zu prüfen. Erkennt Hinoa jedoch ohne vertiefte Prüfung, dass eine Weisung offensichtlich gegen datenschutzrechtliche Vorschriften verstößt, wird Hinoa den Auftraggeber hierauf unverzüglich hinweisen und ist berechtigt, die Ausführung bis zur Klärung auszusetzen.

Produkt- oder Systemeinstellungen, Konfigurationen oder automatisierte Abläufe, die der Auftraggeber eigenständig innerhalb der Hinoa-Dienste vornimmt, gelten als Weisung im Sinne dieses Vertrags. Ebenso gelten mündliche oder sprachbasierte Eingaben des Auftraggebers an den KI-Assistenten als dokumentierte Weisung, soweit diese vom System protokolliert werden. Hinoa ist nicht verpflichtet, solche Einstellungen oder Eingaben fortlaufend zu überwachen oder auf ihre rechtliche Zulässigkeit zu prüfen.

Hinoa verarbeitet die personenbezogenen Daten nach dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO und daher nur so weit, als dies zur Erbringung der vereinbarten Leistungen erforderlich ist.

Speicherdauer und Löschung. Audioinhalte werden ausschließlich flüchtig in Echtzeit verarbeitet und nicht gespeichert. Gesprächstranskripte, Gesprächszusammenfassungen und Protokolle der vom KI-Assistenten ausgeführten Aktionen werden für 90 Tage ab dem jeweiligen Gespräch gespeichert und anschließend automatisiert gelöscht. Kopien, die im Rahmen der Leistungserbringung in Systeme des Auftraggebers (z. B. CRM, E-Mail, Kalender) übertragen wurden, verbleiben dort und sind von dieser Löschung nicht umfasst. Der Auftraggeber kann in Textform (support@hinoa.de) eine abweichende, kürzere oder längere Speicherdauer anweisen. Sicherungskopien werden spätestens 30 Tage nach der Löschung der Primärdaten überschrieben.

Qualitätssicherung und Fehleranalyse. Der Auftraggeber weist Hinoa an, Gesprächstranskripte, Gesprächszusammenfassungen und Aktionsprotokolle durch benannte, zur Vertraulichkeit verpflichtete Mitarbeiter von Hinoa einzusehen, soweit dies zur Fehleranalyse, zur Qualitätssicherung und zur Sicherstellung des vertragsgemäßen Betriebs des KI-Assistenten erforderlich ist. Rufnummern werden in dieser Ansicht maskiert; der Zugriff erfolgt ausschließlich über personalisierte Konten mit Mehr-Faktor-Authentifizierung und wird protokolliert. Erkenntnisse aus dieser Einsicht werden nur in aggregierter oder anonymisierter Form für die Weiterentwicklung des Dienstes verwendet. Eine Nutzung von Auftraggeberdaten zum Training von KI-Modellen findet nicht statt. Der Auftraggeber kann diese Weisung jederzeit in Textform widerrufen; die Einsicht beschränkt sich dann auf die Bearbeitung konkreter Support-Anfragen des Auftraggebers.

Der Zugriff auf personenbezogene Daten des Auftraggebers wird ausschließlich Personen erteilt, welche diesen Zugriff aufgrund vertraglicher oder gesetzlicher Bestimmungen benötigen.

Alle Personen aufseiten von Hinoa, welche Zugriff auf personenbezogene Daten des Auftraggebers haben, sind zur Verschwiegenheit zu verpflichten. Die Verschwiegenheitspflicht bleibt auch nach Beendigung ihrer Tätigkeit für einen angemessenen Zeitraum fortbestehen.

Hinoa ist verpflichtet, alle geeigneten und angemessenen technischen und organisatorischen Maßnahmen zu ergreifen und aufrechtzuerhalten, um die Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten zu gewährleisten. Die implementierten Maßnahmen sind in Anlage 3 beschrieben; weitergehende Nachweise können über contact@hinoa.de angefordert werden.

Hinoa unterstützt den Auftraggeber bei der Einhaltung seiner Verpflichtungen aus der DSGVO, insbesondere in Bezug auf die Rechte der betroffenen Personen (Art. 12–22 DSGVO). Auskunfts-, Berichtigungs- und Löschersuchen zu einzelnen betroffenen Personen bearbeitet Hinoa auf Weisung des Auftraggebers innerhalb von zehn Werktagen.

Hinoa wird ohne vorherige Weisung des Auftraggebers nicht direkt mit betroffenen Personen kommunizieren, es sei denn, Hinoa ist hierzu gesetzlich verpflichtet.

Sofern gesetzliche Bestimmungen nicht entgegenstehen, wird Hinoa den Auftraggeber unverzüglich informieren, wenn eine Information oder Mitteilung in Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen dieses AVV steht.

Meldung von Datenschutzverstößen. Hinoa hat den Auftraggeber unverzüglich, in der Regel innerhalb von 48 Stunden nach Kenntniserlangung, zu informieren, wenn personenbezogene Daten unrechtmäßig verwendet wurden und/oder den Betroffenen Schaden droht. Hinoa stellt alle notwendigen Informationen zur Verfügung, damit der Auftraggeber seinen Meldepflichten nachkommen kann.

Im Verhältnis der Parteien zueinander haftet Hinoa nur für Verstöße gegen diese Vereinbarung, die auf eigenes Verschulden zurückzuführen sind; eine Freistellung für Verstöße des Auftraggebers ist ausgeschlossen. Die gesetzliche Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

Hinoa unterstützt den Auftraggeber bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und bei der Einhaltung von Art. 32 (Sicherheit der Verarbeitung) und Art. 36 (Konsultation der Datenschutzbehörde), soweit technisch möglich und verhältnismäßig. Hinoa stellt dem Auftraggeber hierfür auf Anfrage eine Beschreibung der Verarbeitung sowie die TOM-Dokumentation zur Verfügung.

Jede Übermittlung personenbezogener Daten an ein Drittland erfolgt im Einklang mit den Bestimmungen der DSGVO (Anlage 2).

4. Unterauftragsverarbeiter

Hinoa ist berechtigt, Sub-Auftragsverarbeiter einzusetzen. Änderungen teilt Hinoa in Textform mit; widerspricht der Auftraggeber nicht binnen 14 Kalendertagen ab Versand der Information, gilt der neue Sub-Auftragsverarbeiter als genehmigt.

Im Fall eines Einspruches werden Auftraggeber und Hinoa zur Lösung des Konflikts in Kontakt treten, wobei ein außerordentliches Kündigungsrecht der Hauptvereinbarung für beide Seiten vereinbart wird, falls der Konflikt nicht gelöst werden kann.

Zwischen Hinoa und dem Sub-Auftragsverarbeiter muss ein Vertrag gemäß Art. 28 Abs. 4 DSGVO geschlossen werden, der ein dem Datenschutz- und Sicherheitsniveau dieses Vertrages entsprechendes Schutzniveau gewährleistet.

Hinoa hat die Einhaltung der Datenschutzpflichten durch Sub-Auftragsverarbeiter regelmäßig zu prüfen und den Auftraggeber bei Verstößen umgehend zu informieren.

Die genehmigten Sub-Auftragsverarbeiter ergeben sich aus Anlage 1 in der jeweils aktuellen Fassung dieses AVV. In Anlage 1 als „optional“ gekennzeichnete Sub-Auftragsverarbeiter werden nur eingesetzt, wenn der Auftraggeber die jeweilige Funktion oder Integration konfiguriert oder Hinoa den Einsatz vorab in Textform mitteilt; alle übrigen sind im laufenden Betrieb eingesetzt. Änderungen richten sich nach den vorstehenden Absätzen dieser Ziffer.

5. Prüfung und Einhaltung

Der Auftraggeber ist berechtigt, nach angemessener Vorankündigung Audits zur Überprüfung der Einhaltung dieser Vereinbarung durchzuführen. Audits erfolgen grundsätzlich durch Einsicht in geeignete Nachweise (z.B. TOM-Dokumentation, Zertifikate). Vor-Ort-Audits sind nur bei konkretem Anlass und nach vorheriger Abstimmung zulässig. Die Kosten eines Audits trägt der Auftraggeber.

Hinoa stellt dem Auftraggeber alle erforderlichen Informationen zur Verfügung und arbeitet mit ihm zusammen, um die Einhaltung der DSGVO nachzuweisen.

6. Laufzeit und Beendigung der Auftragsverarbeitung

Dieser AVV tritt mit Annahme des Order Forms in Kraft und gilt für die Dauer der Nutzung der Hinoa-Dienste durch den Auftraggeber. Er kann jederzeit mit Wirkung zum Ende der Nutzung oder mit Kündigung des Hauptvertrags beendet werden.

Dieser AVV gilt eigenständig und unabhängig davon, ob zwischen den Parteien ein weiterer Hauptvertrag besteht. Besteht ein solcher Vertrag, ergänzt dieser AVV dessen Bestimmungen; bei Widersprüchen gehen die Regelungen dieses AVV in datenschutzrechtlichen Fragen vor. Im Übrigen gilt die im Order Form festgelegte Rangfolge.

Nach Beendigung der Verarbeitung löscht oder gibt Hinoa die personenbezogenen Daten gemäß Weisung des Auftraggebers zurück, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Erfolgt keine Weisung, löscht Hinoa die Daten spätestens 30 Tage nach Vertragsende, frühestens jedoch nach Erfüllung eines innerhalb dieser Frist gestellten Herausgabeverlangens gemäß §3 MSA. Die Löschung wird auf Anfrage in Textform bestätigt.

Hinoa ist gleichermaßen verpflichtet, die Vernichtung oder Übergabe durch etwaige Sub-Auftragsverarbeiter herbeizuführen.

7. Verantwortlichkeit des Auftraggebers

Der Auftraggeber ist allein verantwortlich für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Sinne der DSGVO. Hinoa verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und ist nicht verpflichtet, die rechtliche Zulässigkeit einzelner Konfigurationen zu prüfen.

Informationspflichten und eigene Datenschutzerklärung. Der Auftraggeber stellt sicher, dass die Verarbeitung personenbezogener Daten betroffener Personen (insbesondere von Anrufern und Gesprächspartnern) durch die Hinoa-Dienste in seiner eigenen Datenschutzerklärung sowie in seinen Informationspflichten gemäß Art. 13 und 14 DSGVO ordnungsgemäß abgebildet ist. Dazu zählen insbesondere Hinweise auf den KI-gestützten Charakter der Kommunikation, die Verarbeitung durch Sub-Auftragsverarbeiter (vgl. Anlage 1 dieses AVV) sowie etwaige Übermittlungen in Drittländer.

Datenschutz-Folgenabschätzung. Der Auftraggeber prüft eigenverantwortlich, ob der Einsatz des KI-Assistenten in seinem Betrieb eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erfordert; Hinoa unterstützt gemäß Ziffer 3.

Für die weitergehenden Mitwirkungs- und Verantwortlichkeitspflichten des Auftraggebers – insbesondere hinsichtlich der eigenverantwortlichen Konfiguration des Services, KI-generierter Inhalte, Kommunikationsmaßnahmen und sensibler Daten – gelten die Regelungen des Hauptvertrags (insbesondere §5 MSA Mitwirkungspflichten und Verantwortung des Kunden).

8. Datenschutz-Informationen zu diesem Vertrag

Daten aus diesem Vertrag. Im Rahmen der Bereitstellung des Services erhebt Hinoa gemäß Art. 6 Abs. 1 lit. b DSGVO Daten des Auftraggebers sowie dessen Mitarbeiter in Form von Informationen über die Datennutzung, Systemstatistik, Computer- und Netzwerkdaten. Darüber hinaus erfolgt eine Verarbeitung zum Zweck der Erfüllung rechtlicher Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO (z.B. Rechnungslegung). Gemäß Art. 6 Abs. 1 lit. f DSGVO verarbeitet Hinoa personenbezogene Daten zur Dokumentation der Geschäftsbeziehung.

Speicherdauer. Personenbezogene Daten des Auftraggebers werden zum Zweck der Erfüllung gesetzlicher Verpflichtungen gemäß § 147 AO für zumindest sechs Jahre

aufbewahrt. Darüber hinaus findet eine Speicherung bis zu maximal zehn Jahre nach Abschluss der Aufträge statt. Sofern kein Vertragsabschluss erfolgte, werden die Daten für voraussichtlich zwölf Monate aufbewahrt.

Betroffenenrechte. Die für den Auftraggeber handelnden natürlichen Personen haben das Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten, das Recht auf Einschränkung der Datenverarbeitung, das Recht auf Datenübertragbarkeit und das Recht zur Beschwerde bei einer Datenschutzaufsichtsbehörde.

Widerspruchsrecht. Die für den Auftraggeber handelnden natürlichen Personen haben das Recht, der Verarbeitung ihrer personenbezogenen Daten gemäß Art. 6 Abs. 1 lit. f DSGVO zu widersprechen. Im Fall des Widerspruchs werden seine personenbezogenen Daten nicht mehr zum Zweck der Direktwerbung verarbeitet.

9. Schlussbestimmungen

Es gilt das Recht der Bundesrepublik Deutschland.

Gerichtsstand für alle Streitigkeiten ist, soweit zulässig, Berlin.

Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Dieser AVV wird mit Annahme des Order Forms Vertragsbestandteil; eine gesonderte Unterzeichnung ist nicht erforderlich, sofern keine der Parteien dies ausdrücklich verlangt. Der Anbieter veröffentlicht die jeweils aktuelle Fassung dieses AVV und stellt sie dem Auftraggeber auf Anfrage zur Verfügung.

Anlage 1 – Genehmigte Unterauftragsverarbeiter (Stand: 17. August 2026)

Anbieter	Beschreibung / Zweck	Datenstandorte	Rechtsgrundlage Drittland
Amazon Web Services EMEA SARL	Cloud-Infrastruktur (Betrieb des Sprachassistenten, Sicherungen)	EU; USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
Supabase Inc.	Datenbank, Authentifizierung, Speicherung von Transkripten und Konfigurationen	EU; USA (Support- und Administrationszugriff möglich)	EU SCC
Vercel Inc.	Hosting der Web-Anwendung und Schnittstellen	EU; USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
Twilio Inc.	Telefonie (Rufnummern, ein- und ausgehende Anrufe); Rufnummern in EU-Region, ausgehende Anrufe teilweise über US-Infrastruktur	EU, EWR, USA	EU SCC; ergänzend EU-US DPF
LiveKit Inc.	Echtzeit-Audioübertragung (SIP/WebRTC) zwischen Telefonie und Sprachassistent	EU, EWR, USA	EU SCC; ergänzend EU-US DPF
Google Ireland Ltd	Cloud-Arbeitsumgebung, E-Mail, Kalender (optional Integration des Auftraggebers)	EU, EWR; USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
Resend Inc.	Transaktions-E-Mails	EU, EWR; USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
OpenAI Ireland Ltd (Verarbeitung durch OpenAI OpCo, LLC, USA, als deren Unterauftragsverarbeiter)	Echtzeit-Sprachverarbeitung des KI-Assistenten; flüchtige Verarbeitung, keine Speicherung von Audio, keine Trainingsnutzung	Vertragspartner EU; Verarbeitung USA	Konzerninterne EU SCC (OpenAI Ireland → OpenAI OpCo)

Anbieter	Beschreibung / Zweck	Datenstandorte	Rechtsgrundlage Drittland
Datadog Inc.	Monitoring, Protokollierung und Fehleranalyse der Infrastruktur	EU (Datadog EU-Site); USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
Microsoft Ireland Operations Ltd	Cloud-Infrastruktur, KI-Sprach- und LLM-Verarbeitung (Azure / Azure AI Foundry); Outlook- und Kalender-Integration (optional)	EU, EWR; USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
Deepgram Inc.	Speech-to-Text (optional)	USA	EU SCC; ergänzend EU-US DPF
ElevenLabs Inc.	Speech-to-Text und Text-to-Speech (optional)	EU, EWR; USA (Support- und Administrationszugriff möglich)	EU SCC; ergänzend EU-US DPF
Cartesia AI Inc.	Text-to-Speech (optional)	USA	EU SCC
Telnyx LLC / Telnyx Ireland Ltd	Telefonie (optional)	EU, EWR	EU SCC

Legende: „(optional)“ = Einsatz nur nach Konfiguration durch den Auftraggeber oder Mitteilung nach Ziffer 4; alle übrigen Anbieter sind im laufenden Betrieb eingesetzt. Die Angabe der Datenstandorte umfasst auch einen möglichen Zugriff aus Drittländern zu Support- und Administrationszwecken. Standardvertragsklauseln (SCC) sind in allen Fällen die primäre Übermittlungsgrundlage; eine Zertifizierung nach dem EU-US Data Privacy Framework wird ergänzend berücksichtigt. Zertifizierungsstatus und Rechtsgrundlagen werden regelmäßig überprüft; der jeweils aktuelle Stand wird auf Anfrage mitgeteilt.

Anlage 2 – Internationale Übermittlungen und ergänzende Maßnahmen

Gesprächsdaten (Transkripte, Zusammenfassungen, Aktionsprotokolle, Konfigurationen) werden ausschließlich in der EU gespeichert. Die Echtzeit-Sprachverarbeitung und -Audioübertragung laufen derzeit über Infrastruktur in den USA, flüchtig und ohne Speicherung; ausgehende Anrufe (Noa Outbound) können teilweise über US-Infrastruktur geleitet werden. Bei US-Anbietern mit EU-Hosting ist ein Support-Zugriff aus den USA möglich. Übermittlungen an Anbieter mit Sitz in Drittländern (insbesondere USA) erfolgen ausschließlich auf Grundlage der EU-Standardvertragsklauseln (SCC, Modul 3) und ergänzender technischer und organisatorischer Maßnahmen; für jeden Sub-Auftragsverarbeiter mit Drittlandbezug liegt ein Transfer Impact Assessment vor, das

jährlich sowie anlassbezogen überprüft wird. Einzelheiten je Anbieter ergeben sich aus Anlage 1. Zu den ergänzenden Maßnahmen zählen insbesondere::

- Keine Speicherung von Audioinhalten: Sprachdaten werden ausschließlich flüchtig in Echtzeit verarbeitet.
- Datenminimierung: An KI-Sub-Auftragsverarbeiter werden nur die für das jeweilige Gespräch erforderlichen Inhalte übermittelt; keine Übermittlung des gesamten Kundenbestands.
- Verschlüsselung der personenbezogenen Daten im Transit (TLS 1.2+) und im Ruhezustand (AES-256) bei allen Sub-Auftragsverarbeitern.
- Keine Nutzung von Auftraggeberdaten zum Training oder zur Verbesserung der Modelle durch die KI-Sub-Auftragsverarbeiter (vertraglich ausgeschlossen, API-Nutzung ohne Datenfreigabe). Der KI-Anbieter speichert Ein- und Ausgaben nach eigenen Angaben ausschließlich zur Missbrauchskontrolle für bis zu 30 Tage; darüber hinaus erfolgt keine Speicherung, vorbehaltlich gesetzlicher Aufbewahrungspflichten.
- Bevorzugung von EU-Datenstandorten, soweit vom Anbieter angeboten; die Umstellung der Echtzeit-Sprachverarbeitung auf EU-Datenresidenz wird angestrebt.
- Soweit US-Anbieter im Rahmen des EU-US Data Privacy Frameworks zertifiziert sind, wird dies ergänzend als Rechtsgrundlage herangezogen; die SCC bleiben auch in diesem Fall vereinbart.

Anlage 3 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Hinoa hält die nachstehenden Maßnahmen aufrecht und passt sie dem Stand der Technik an, ohne das vereinbarte Schutzniveau zu unterschreiten. Die ausführliche TOM-Dokumentation in der jeweils aktuellen Fassung ist Bestandteil dieser Anlage und wird dem Auftraggeber auf Anfrage über contact@hinoa.de zur Verfügung gestellt.

Vertraulichkeit. Betrieb ausschließlich in ISO-27001- bzw. SOC-2-zertifizierten Rechenzentren der in Anlage 1 genannten Cloud-Anbieter in der EU (Datenbank, Sicherungen, Anwendung). Zugang zu Produktionssystemen nur über personalisierte Konten mit Mehr-Faktor-Authentifizierung nach dem Prinzip der minimalen Rechte; alle Zugriffsberechtigten sind zur Vertraulichkeit verpflichtet. Daten verschiedener Auftraggeber werden durch Mandantenkennung und Zugriffsrichtlinien auf Datenbankebene logisch getrennt. Zugangsdaten zu Drittsystemen des Auftraggebers werden verschlüsselt gespeichert.

Integrität. Verschlüsselung aller Datenübertragungen (TLS) und der gespeicherten Daten (AES-256). Audioinhalte werden nicht gespeichert. Aktionen des KI-Assistenten und administrative Zugriffe auf Auftraggeberdaten werden protokolliert.

Verfügbarkeit. Tägliche verschlüsselte Sicherung der Datenbank in der EU; laufende Überwachung der Systeme mit Alarmierung; Notfallkonzept.

Verfahren zur Überprüfung. Verzeichnis der Verarbeitungstätigkeiten, Löschkonzept (Ziffer 3), dokumentierter Prozess für Datenschutzvorfälle, jährliche Überprüfung der Maßnahmen und der Sub-Auftragsverarbeiter (Ziffer 4), Schulung der Mitarbeiter.

KI-gestützte Verarbeitung. Keine Nutzung von Auftraggeberdaten zum Training von KI-Modellen; der Assistent führt ausschließlich definierte, protokollierte Aktionen aus; Drittlandübermittlungen nach Anlage 2.