

Vertrag über die Auftragsverarbeitung (AVV)

gemäß Art. 28 Abs. 3 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO)

zwischen

{{kunde.firma}}

— nachfolgend „**Auftraggeber**“ (Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO) —

und

Nurion Application 1 GmbH

Harkortstraße 95, 22765 Hamburg

vertreten durch: Dr. Johannes Jacubeit

— nachfolgend „**Auftragnehmer**“ (Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO) —

Auftraggeber und Auftragnehmer gemeinsam die „**Parteien**“.

Präambel

Der Auftragnehmer betreibt die Software „karlo“, eine cloudbasierte Anwendung zur digitalen Fallbearbeitung für Kfz-Sachverständigen-Büros (nachfolgend der „**Dienst**“). Der Auftraggeber nutzt den Dienst auf Grundlage des zwischen den Parteien geschlossenen Nutzungsvertrags (nachfolgend der „**Hauptvertrag**“). Im Rahmen der Nutzung des Dienstes verarbeitet der Auftragnehmer personenbezogene Daten — insbesondere Daten von Unfallbeteiligten und weiteren am Schadenfall beteiligten Personen — ausschließlich im Auftrag und nach Weisung des Auftraggebers. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus Art. 28 DSGVO.

§ 1 Gegenstand und Dauer des Vertrags

1. Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Rahmen der Bereitstellung und des Betriebs des Dienstes gemäß Hauptvertrag.
2. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags gilt zugleich als Kündigung dieses Vertrags zum selben Zeitpunkt. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen, solange der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.
3. Die Pflichten aus § 10 (Löschung und Rückgabe) bestehen über das Vertragsende hinaus fort, bis sie vollständig erfüllt sind.

§ 2 Art und Zweck der Verarbeitung

1. **Art der Verarbeitung:** Erhebung, Erfassung, Organisation, Ordnung, Speicherung, Anpassung, Auslesen, Abfragen, Verwendung, Übermittlung an vom Auftraggeber bestimmte Empfänger (z. B. Anwälte, Werkstätten, Versicherer), Verknüpfung, Einschränkung, Löschung und Vernichtung personenbezogener Daten — jeweils ganz oder teilweise automatisiert.
2. **Zweck der Verarbeitung:** Digitale Anlage, Bearbeitung, Dokumentation und Abwicklung von Kfz-Schadenfällen des Auftraggebers, einschließlich: Fallakte und Falldokumentation; Aufnahme und Transkription von Kundengesprächen nach vorheriger Einwilligung der betroffenen Person; KI-gestützte Erstellung von Text- und Gutachtenentwürfen (die fachliche Prüfung und Freigabe verbleibt stets beim Auftraggeber); Erstellung, Versand und Archivierung von Dokumenten und Schriftverkehr; Bereitstellung eines Zugangs für Unfallkunden über personalisierte Zugriffslinks (Magic-Link).
3. Die Verarbeitung findet ausschließlich in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum statt. Ausnahmen gelten nur nach Maßgabe von § 7 (Drittlandtransfer).

§ 3 Kategorien personenbezogener Daten

1. Gegenstand der Verarbeitung sind folgende Datenkategorien:
 - **Stammdaten der Unfallbeteiligten:** Name, Anschrift, Kontaktdaten (Telefon, E-Mail), Geburtsdatum, Rolle im Schadenfall (Geschädigter, Unfallgegner, Zeuge);
 - **Fahrzeug- und Kennzeichendaten:** amtliches Kennzeichen, Fahrzeug-Identifizierungsnummer (FIN), Fahrzeugtyp, Halterdaten, Zulassungsdaten;
 - **Schadenfalldaten:** Unfallhergang, Schadensbeschreibung, Besichtigungsdaten, Kalkulations- und Bewertungsdaten, Gutachten und Gutachtenentwürfe;
 - **Fotos und Bilddokumentation:** Lichtbilder von Fahrzeugen, Schäden und Unfallörtlichkeit; auf Fotos können Personen, Kennzeichen und Umgebungsmerkmale erkennbar sein;
 - **Gesprächsaufzeichnungen und Transkripte:** Audioaufnahmen von Kundengesprächen (nur nach dokumentierter Einwilligung der betroffenen Person) sowie daraus erzeugte Transkripte und Diktate;
 - **Kommunikationsdaten:** Schriftverkehr mit Unfallbeteiligten, Anwälten, Werkstätten und Versicherern;
 - **Vertrags- und Abrechnungsdaten des Auftraggebers:** Rechnungs- und Honorardaten je Fall;
 - **Nutzungs- und Protokolldaten:** Log-Daten der Nutzerkonten des Auftraggebers, Audit-Ereignisse der Fallbearbeitung.
2. **Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO):** Unfallschilderungen, Gesprächsaufzeichnungen, Transkripte und Schriftverkehr können Angaben zu

Verletzungen, Heilbehandlungen oder sonstige Gesundheitsdaten der Unfallbeteiligten enthalten (Art. 9 Abs. 1 DSGVO). Die Parteien vereinbaren hierzu: (a) Der Auftragnehmer verarbeitet solche Daten ausschließlich als unselbständigen Bestandteil der Falldokumentation und wertet sie nicht eigenständig aus. (b) Der Auftraggeber ist dafür verantwortlich, dass für die Verarbeitung dieser Daten eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO besteht (insbesondere Art. 9 Abs. 2 lit. f DSGVO — Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen — oder eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO). (c) Auf diese Daten finden die technischen und organisatorischen Maßnahmen der Anlage 1 in vollem Umfang Anwendung, einschließlich Verschlüsselung bei Übertragung und Speicherung.

§ 4 Kategorien betroffener Personen

- Unfallbeteiligte (Geschädigte, Unfallgegner, Fahrzeughalter, Zeugen), einschließlich der Unfallkunden mit Zugriff über Magic-Link;
- Beschäftigte und Nutzer des Auftraggebers (Büro-Nutzer);
- Ansprechpersonen bei Anwaltskanzleien, Werkstätten, Versicherern und sonstigen am Schadenfall beteiligten Stellen.

§ 5 Pflichten des Auftragnehmers

1. **Weisungsbindung (Art. 28 Abs. 3 lit. a DSGVO):** Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation —, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Hauptvertrag, dieser Vertrag und die Nutzung der Funktionen des Dienstes durch den Auftraggeber gelten als dokumentierte Weisungen. Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, bedürfen der Textform.
2. **Hinweis auf rechtswidrige Weisungen (Art. 28 Abs. 3 UAbs. 2 DSGVO):** Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung so lange auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.
3. **Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO):** Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeitspflicht besteht nach Beendigung der Tätigkeit fort.

4. Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO):

Der Auftragnehmer ergreift alle nach Art. 32 DSGVO erforderlichen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses implementierten technischen und organisatorischen Maßnahmen sind in **Anlage 1** beschrieben. Der Auftragnehmer darf diese Maßnahmen an den Stand der Technik anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

5. Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 lit. e DSGVO): Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Kapitel III der DSGVO (Art. 12 bis 23 DSGVO) nachzukommen. Macht eine betroffene Person Rechte unmittelbar gegenüber dem Auftragnehmer geltend, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter.

6. Unterstützung bei Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO): Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere:

- **Meldung von Verletzungen (Art. 33 DSGVO):** Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden, in Textform an die vom Auftraggeber benannte Kontaktadresse. Die Meldung enthält, soweit verfügbar, die Angaben nach Art. 33 Abs. 3 DSGVO.
- **Benachrichtigung betroffener Personen (Art. 34 DSGVO):** Der Auftragnehmer stellt dem Auftraggeber die für eine Benachrichtigung erforderlichen Informationen zur Verfügung.
- **Datenschutz-Folgenabschätzung (Art. 35, 36 DSGVO):** Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die für eine Datenschutz-Folgenabschätzung und eine etwaige vorherige Konsultation der Aufsichtsbehörde erforderlichen Informationen über die Verarbeitung im Dienst zur Verfügung.

7. Verzeichnis von Verarbeitungstätigkeiten: Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

8. Datenschutzbeauftragter: Soweit der Auftragnehmer zur Benennung eines Datenschutzbeauftragten verpflichtet ist, benennt er diesen und teilt dem Auftraggeber die Kontaktdaten mit. Ansprechstelle für Datenschutzfragen ist: karlo@nurion.com.

§ 6 Unterauftragsverarbeiter

1. Allgemeine Genehmigung (Art. 28 Abs. 2 DSGVO): Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung zur Einschaltung weiterer Auftragsverarbeiter

(Unterauftragsverarbeiter). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in **Anlage 2** aufgeführt; ihr Einsatz gilt als genehmigt.

2. **Informationspflicht und Widerspruchsrecht:** Der Auftragnehmer informiert den Auftraggeber vorab in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters, mindestens 30 Tage vor Wirksamwerden der Änderung. Der Auftraggeber kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Im Fall eines berechtigten Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung; kommt eine solche nicht zustande, ist jede Partei berechtigt, den Hauptvertrag mit einer Frist von einem Monat zum Monatsende zu kündigen.
3. **Vertragliche Weitergabe der Pflichten (Art. 28 Abs. 4 DSGVO):** Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragsverarbeiters.
4. Nicht als Unterauftragsverarbeitung gelten Nebenleistungen ohne inhaltlichen Bezug zu den Auftragsdaten (z. B. Telekommunikationsleistungen, Wartung von Betriebssystemen, Entsorgung von Datenträgern), sofern der Zugriff auf Auftragsdaten ausgeschlossen ist oder ausschließlich verschlüsselte Daten ohne Schlüsselzugriff betroffen sind.

§ 7 Verarbeitung in Drittländern; KI-Dienste

1. Die Verarbeitung erfolgt grundsätzlich in der EU bzw. dem EWR (§ 2 Abs. 3).
2. **KI-gestützte Entwurfserstellung:** Für die KI-gestützte Erstellung von Text- und Gutachtenentwürfen sowie die Transkription setzt der Auftragnehmer Anbieter großer Sprachmodelle (LLM-Anbieter) als Unterauftragsverarbeiter ein (Anlage 2). Einzelne dieser Anbieter haben ihren Sitz in den Vereinigten Staaten von Amerika; bei ihrer Nutzung kann eine Übermittlung personenbezogener Daten in die USA stattfinden (Drittlandtransfer i. S. d. Art. 44 ff. DSGVO).
3. **Garantien (Art. 44 ff. DSGVO):** Übermittlungen in Drittländer erfolgen ausschließlich auf Grundlage geeigneter Garantien, nämlich (a) eines Angemessenheitsbeschlusses der Europäischen Kommission nach Art. 45 DSGVO — für US-Anbieter insbesondere des Angemessenheitsbeschlusses zum EU-U.S. Data Privacy Framework (DPF), sofern der jeweilige Anbieter unter dem DPF zertifiziert ist — oder (b) der Standardvertragsklauseln der Europäischen Kommission nach Art. 46 Abs. 2 lit. c DSGVO (Durchführungsbeschluss (EU) 2021/914) einschließlich einer Prüfung und erforderlichenfalls ergänzender Maßnahmen (Transfer Impact Assessment). Die je Unterauftragsverarbeiter einschlägige Garantie ist in Anlage 2 ausgewiesen.

4. **Datenminimierung gegenüber LLM-Anbietern:** Der Auftragnehmer übermittelt an LLM-Anbieter nur die für die jeweilige Entwurfs- oder Transkriptionsleistung erforderlichen Inhalte. Der Auftragnehmer vereinbart mit den LLM-Anbietern, soweit angeboten, dass übermittelte Inhalte nicht zum Training von Modellen verwendet werden.
5. **EU-Routen als benanntes Pilot-Ziel:** Der Wechsel der KI-Verarbeitung auf ausschließlich in der EU betriebene Verarbeitungsrouten (EU-Routen) ist ein benanntes Exit-Kriterium der Pilotphase des Dienstes (karlo#150). Der Auftragnehmer informiert den Auftraggeber über die Umstellung; mit ihrer Umsetzung entfällt der Drittlandtransfer nach Abs. 2 für die betreffenden Verarbeitungen.

§ 8 Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 lit. h DSGVO)

1. Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind.
2. Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags zu überprüfen. Der Nachweis kann in erster Linie erbracht werden durch: aktuelle Testate oder Berichte unabhängiger Prüfer, geeignete Zertifizierungen (z. B. nach Art. 42 DSGVO oder ISO/IEC 27001), Selbstauskünfte des Auftragnehmers oder die Dokumentation der Maßnahmen nach Anlage 1.
3. Soweit im Einzelfall darüber hinaus eine Inspektion erforderlich ist, ermöglicht der Auftragnehmer dem Auftraggeber oder einem von diesem beauftragten, zur Verschwiegenheit verpflichteten Prüfer nach angemessener Vorankündigung (mindestens 14 Tage, außer bei konkreten Anhaltspunkten für Verstöße) während der üblichen Geschäftszeiten Prüfungen im erforderlichen Umfang. Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie Daten anderer Kunden bleiben geschützt.
4. Prüfungen nach Abs. 3 erfolgen höchstens einmal pro Kalenderjahr, es sei denn, ein konkreter Anlass (insbesondere eine Datenschutzverletzung) rechtfertigt eine weitere Prüfung. Der Auftragnehmer kann für die Unterstützung von Prüfungen ohne konkreten Anlass eine angemessene Vergütung verlangen.

§ 9 Löschung und Rückgabe (Art. 28 Abs. 3 lit. g DSGVO)

1. Kopien oder Duplikate der Auftragsdaten werden ohne Wissen des Auftraggebers nicht erstellt; hiervon ausgenommen sind Sicherheitskopien (Backups) sowie Daten, deren Aufbewahrung gesetzlich vorgeschrieben ist.
2. Nach Beendigung des Hauptvertrags gibt der Auftragnehmer nach Wahl des Auftraggebers sämtliche im Auftrag verarbeiteten personenbezogenen Daten in einem gängigen, strukturierten Format zurück (Export) oder löscht sie, einschließlich vorhandener Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Pflicht zur Speicherung besteht. Der Auftraggeber übt sein Wahlrecht innerhalb von 90 Tagen nach Vertragsende in Textform aus; äußert er sich nicht, löscht der Auftragnehmer die Daten nach Ablauf dieser Frist.

3. **Gesetzliche Aufbewahrungspflichten:** Von der Löschpflicht ausgenommen sind Daten und Unterlagen, die der Auftragnehmer aufgrund gesetzlicher Aufbewahrungspflichten — insbesondere § 147 der Abgabenordnung (AO) und § 257 des Handelsgesetzbuchs (HGB) — weiter speichern muss (namentlich abrechnungs- und buchführungsrelevante Datensätze). Solche Daten werden für die weitere Verarbeitung gesperrt und nach Ablauf der jeweiligen Aufbewahrungsfrist gelöscht.
4. Die Löschung aus produktiven Systemen erfolgt unverzüglich; die Löschung aus rotierenden Sicherheitskopien erfolgt mit deren regulärem Überschreibungszyklus gemäß Anlage 1. Der Auftragnehmer bestätigt die Löschung auf Anfrage in Textform.
5. Für die automatisierte fristgebundene Löschung einzelner Artefaktklassen während der Vertragslaufzeit (z. B. Gesprächsaufnahmen) gelten die im Dienst konfigurierten Aufbewahrungsklassen; deren Fristen dürfen gesetzliche Mindestaufbewahrungsfristen nicht unterschreiten.

§ 10 Haftung

1. Für die Haftung der Parteien gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags.
2. Die Parteien stellen einander von der Haftung frei, soweit eine Partei nachweist, dass sie für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, in keinerlei Hinsicht verantwortlich ist (Art. 82 Abs. 3 DSGVO).

§ 11 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform (Art. 28 Abs. 9 DSGVO); dies gilt auch für die Änderung dieser Klausel. Der Abschluss und Änderungen dieses Vertrags können in einem elektronischen Format erfolgen, einschließlich der Zustimmung im Dienst (Consent-Mechanik).
2. **Versionsstand und Re-Consent:** Dieser Vertrag trägt den Versionsstand `{{version}}` vom `{{datum}}`. Bei einer neuen Version dieses Vertrags — insbesondere nach Abschluss der juristischen Prüfung (karlo#139) — informiert der Auftragnehmer den Auftraggeber und holt dessen erneute Zustimmung über den Dienst ein; die dokumentierte Zustimmung des Auftraggebers bezieht sich stets auf eine konkrete Dokumentenversion.
3. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen dieses Vertrags vor.
4. Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.
5. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum: `{{datum}}`

Für den Auftraggeber: _____ ({{kunde.firma}})

Für den Auftragnehmer: _____ (Nurion Application 1 GmbH, Dr. Johannes Jacubeit)

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Stand: {{datum}} · Version {{version}}

1. Zutrittskontrolle (physischer Zugang)

- Der Dienst wird in Rechenzentren eines EU-Hosting-Providers (Anlage 2) betrieben; der physische Zutritt ist durch den Provider gesichert (Zutrittskontrollsysteme, Videoüberwachung, Besucherprotokollierung, 24/7-Sicherheitsdienst; nachgewiesen durch Zertifizierungen des Providers, z. B. ISO/IEC 27001).
- Der Auftragnehmer selbst betreibt keine eigenen Serverräume mit Auftragsdaten. Mobile Endgeräte der Beschäftigten sind vollverschlüsselt und mit Bildschirmsperre versehen.

2. Zugangskontrolle (Systemzugang)

- Zugang zu Produktivsystemen nur für namentlich benannte, autorisierte Beschäftigte über personenbezogene Konten; keine Sammelkonten.
- Multi-Faktor-Authentisierung für administrative Zugänge und für den Zugang zur Cloud-Infrastruktur.
- Passwort-Mindestanforderungen; zentrale Verwaltung und Entzug von Zugängen beim Ausscheiden von Beschäftigten (Offboarding-Checkliste).
- Nutzerzugang zum Dienst über individuelle Konten des Auftraggebers; Unfallkunden erhalten zeitlich begrenzte, personalisierte Zugriffslinks (Magic-Link) mit fallbezogenem, minimalem Berechtigungsumfang.

3. Zugriffskontrolle (Berechtigungen)

- Rollen- und Rechtekonzept nach dem Need-to-know-Prinzip; Zugriffe auf Falldaten sind auf die Organisation (Büro) des Auftraggebers beschränkt.
- Administrative Zugriffe auf Produktivdaten werden protokolliert; Support-Zugriffe erfolgen nur anlassbezogen.
- Protokollierung sicherheitsrelevanter Ereignisse (Audit-Events) in einem manipulationsgeschützten, anfügenden (append-only) Ereignisprotokoll.

4. Trennungskontrolle

- Mandantentrennung auf Anwendungsebene: jede Abfrage ist an die Organisation des Auftraggebers gebunden; Falldaten verschiedener Kunden werden logisch getrennt verarbeitet.
- Trennung von Produktiv-, Test- und Entwicklungsumgebungen; keine Produktivdaten in Test- oder Entwicklungsumgebungen.

5. Pseudonymisierung und Datenminimierung

- Übermittlungen an KI-Dienste werden auf die für die jeweilige Leistung erforderlichen Inhalte beschränkt (§ 7 Abs. 4 AVV).
- Lösch-Nachweise (Tombstone-Ereignisse) enthalten keine Inhaltsdaten und keine personenbezogenen Dateinamen.
- Interne Auswertungen erfolgen, soweit möglich, mit aggregierten oder pseudonymisierten Daten.

6. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Transportverschlüsselung: sämtliche Verbindungen zum Dienst und zwischen Dienstkomponenten sind mit TLS (mindestens Version 1.2) verschlüsselt.
- Speicherverschlüsselung: Datenbanken, Objektspeicher (Fotos, Aufnahmen, Dokumente) und Backups sind at rest verschlüsselt (AES-256 oder gleichwertig).
- Schlüsselverwaltung über die Schlüsselverwaltungsdienste des EU-Hosting-Providers; Zugriff auf Schlüssel ist auf das erforderliche Minimum beschränkt.

7. Verfügbarkeitskontrolle und Belastbarkeit

- Tägliche automatisierte Backups mit definierter Aufbewahrung; regelmäßige Wiederherstellungstests.
- Redundante Infrastruktur des Hosting-Providers; Überwachung (Monitoring) und Alarmierung für Verfügbarkeit und Fehlerzustände.
- Dokumentiertes Vorgehen für Sicherheitsvorfälle (Incident-Response) einschließlich der Meldewege nach § 5 Abs. 6 AVV.
- Zeitnahes Einspielen von Sicherheitsaktualisierungen (Patch-Management); Absicherung der Software-Lieferkette durch Versionskontrolle und automatisierte Prüfungen (CI).

8. Auftragskontrolle

- Schriftliche Verträge nach Art. 28 Abs. 4 DSGVO mit sämtlichen Unterauftragsverarbeitern (Anlage 2); Prüfung der Garantien vor Beauftragung.

- Weisungen des Auftraggebers werden über den Hauptvertrag, diesen Vertrag und die Funktionen des Dienstes dokumentiert.
- Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO), mindestens jährlich sowie anlassbezogen.

9. Löschkonzept

- Aufbewahrungsklassen je Artefakttyp mit fristgebundener automatisierter Löschung nach Fallabschluss; gesetzliche Mindestaufbewahrungsfristen (§ 147 AO, § 257 HGB) werden systemseitig nie unterschritten.
- Gesprächsaufnahmen und Roh-Transkripte werden standardmäßig 90 Tage nach Fallabschluss automatisiert gelöscht.
- Jede automatisierte Löschung erzeugt einen inhaltsfreien Lösch-Nachweis (Tombstone-Ereignis); ein fallbezogener Legal Hold blockiert jede Löschung.

Anlage 2 — Genehmigte Unterauftragsverarbeiter

Stand: {{datum}} · Version {{version}}

Unterauftragsverarbeiter	Zweck der Verarbeitung	Sitz / Verarbeitungsort	Garantie bei Drittlandtransfer
{{subprozessor.hosting.name}}	Hosting, Datenbank- und Objektspeicher-Betrieb (EU-Hosting-Provider)	{{subprozessor.hosting.sitz}} (EU)	— (keine Drittlandübermittlung)
{{subprozessor.llm.name}} (Anthropic PBC / OpenAI, L.L.C. / Google LLC)	KI-gestützte Entwurfserstellung (Text- und Gutachtenentwürfe)	USA	EU-U.S. Data Privacy Framework (DPF), soweit zertifiziert; im Übrigen Standardvertragsklausel in (Art. 46 Abs. 2 lit. c DSGVO)
{{subprozessor.transkription.name}}	Transkription von Gesprächsaufnahmen	{{subprozessor.transkription.sitz}}	{{subprozessor.transkription.garantie}}
{{subprozessor.email.name}}	Transaktionaler E-Mail-Versand (z. B. Magic-Links, Benachrichtigungen)	{{subprozessor.email.sitz}}	{{subprozessor.email.garantie}}
LetterXpress GmbH	Postalischer Brief-Versand (Druck,	Deutschland	— (keine Drittlandübermittlung)

Unterauftragsverarbeiter	Zweck der Verarbeitung	Sitz / Verarbeitungsort	Garantie bei Drittlandtransfer
	Kuvertierung, Zustellung)		

Hinweis: Der Wechsel der KI-Verarbeitung auf EU-Routen ist ein benanntes Exit-Kriterium der Pilotphase (karlo#150, § 7 Abs. 5 AVV). Nach der Umstellung wird diese Anlage aktualisiert; es gilt das Verfahren nach § 6 Abs. 2 AVV.

ENTWURF — rechtliche Prüfung ausstehend (karlo#139)