RECHTLICHES

Auftragsverarbeitungsvertrag (AVV)

Teil der Nutzungsbedingungen, Version 2.12 · Gültig ab 13. November 2026

Dieser Vertrag ist Teil der Nutzungsbedingungen von Korpus. Er gilt automatisch, sobald Sie für ein Unternehmen oder eine andere Organisation personenbezogene Daten anderer Personen in einem Team mit bezahltem Plan ablegen; eine Unterschrift ist nicht nötig. Für die rein private Nutzung gilt er nicht. Die deutsche Fassung ist verbindlich. English translation · PDF dieser Fassung

§ 1 Parteien, Gegenstand, Dauer

(1) Dieser Vertrag gilt zwischen dem Anbieter von Korpus (Auftragsverarbeiter, Anlage 1) und der Nutzerin oder dem Nutzer von Korpus, die oder der in Bundles eines Teams mit bezahltem Plan (Pro oder Business) personenbezogene Daten für Zwecke verarbeitet, die nicht ausschließlich persönlich oder familiär sind (Art. 2 Abs. 2 lit. c DSGVO), als Verantwortlichem ("Kunde"). Wer Korpus für ein Unternehmen oder eine andere Organisation nutzt, schließt diesen Vertrag für diese ab und versichert, dazu berechtigt zu sein; sie ist dann der Kunde. Für Teams im kostenlosen Plan gilt dieser Vertrag nicht; dort legt der Kunde für solche Zwecke keine personenbezogenen Daten anderer Personen ab (§ 6 der Nutzungsbedingungen).

(2) Der Vertrag wird mit der Annahme der Nutzungsbedingungen in elektronischem Format geschlossen (Art. 28 Abs. 9 DSGVO). Er gilt für den vom Anbieter betriebenen Dienst unter `korpus.cloud`. Für Korpus in einer eigenen Instanz oder im eigenen AWS-Konto des Kunden (Business) gilt ein gesonderter Vertrag.

(3) Gegenstand ist die Bereitstellung von Korpus nach den Nutzungsbedingungen. Dabei verarbeitet der Anbieter die Inhalte, die der Kunde in den Bundles dieser Teams ablegt, in dessen Auftrag.

(4) Der Vertrag gilt, solange ein Team des Kunden einen bezahlten Plan hat, und danach für die bis dahin abgelegten Daten weiter, bis der Kunde sie gelöscht hat; spätestens endet er mit dem Nutzungsvertrag. § 4 Abs. 1 (Vertraulichkeit) und § 10 (Löschung) gelten darüber hinaus.

§ 2 Art und Zweck, Daten, Betroffene

(1) **Art der Verarbeitung:** Speichern, Ordnen, Anzeigen, Durchsuchen, Verknüpfen, Kopieren, Exportieren und Löschen von Inhalten sowie deren Bereitstellung an die Personen, Teams, Agenten und verbundenen Apps, denen der Kunde Zugriff gibt.

(2) **Zweck:** die Bereitstellung von Korpus und Support auf Anfrage des Kunden. Wofür der Anbieter Bundles als eigener Verantwortlicher öffnet und Inhalte automatisiert prüft, regeln § 3 Abs. 4 und 6.

(3) **Arten von Daten:** alle personenbezogenen Daten, die der Kunde oder in seinem Auftrag Mitglieder, Agenten und Apps in Bundles ablegen: Texte, Dateien und ihre Metadaten, etwa Relationen, Tags und Erwähnungen, dazu das Änderungsprotokoll der Bundles (wer wann was geändert hat). Besondere Kategorien nach Art. 9 DSGVO dürfen nicht abgelegt werden (§ 8 der Nutzungsbedingungen).

(4) **Betroffene:** Personen, deren Daten der Kunde ablegt, typischerweise Beschäftigte, Kunden, Interessenten, Lieferanten und Geschäftspartner des Kunden und deren Ansprechpersonen, sowie Mitglieder seiner Teams und Personen, mit denen er Bundles teilt.

(5) Nicht Gegenstand dieses Vertrags sind die Konto-, Abrechnungs-, Audit- und Sicherheitsdaten, die der Anbieter als eigener Verantwortlicher verarbeitet; dafür gilt die Datenschutzerklärung.

§ 3 Weisungen

(1) Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, auch bei Übermittlungen in Drittländer (Art. 28 Abs. 3 lit. a DSGVO). Weisungen sind dieser Vertrag und die Nutzung von Korpus durch den Kunden und die von ihm Berechtigten. Ist der Anbieter gesetzlich zu einer anderen Verarbeitung verpflichtet, teilt er dem Kunden dies vorher mit, sofern das Gesetz es nicht verbietet.

(2) Weitere Weisungen erteilt der Kunde in Textform an me@till-it-works.de. Was über die Funktionen von Korpus hinausgeht, vereinbaren die Parteien gesondert.

(3) Ist der Anbieter der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, informiert er den Kunden unverzüglich. Er darf die Ausführung aussetzen, bis der Kunde sie bestätigt oder ändert.

(4) Der Anbieter öffnet Bundles nur lesend und nur in den Fällen des § 6 der Nutzungsbedingungen. Auf Bitte des Kunden (Support) handelt er dabei auf dessen Weisung. Für die Sicherheit des Dienstes, gegen Missbrauch oder rechtswidrige Inhalte, zur Erfüllung einer gesetzlichen Pflicht und zur Prüfung einer eingereichten Veröffentlichung öffnet er Bundles als eigener Verantwortlicher, soweit es dafür erforderlich ist (Datenschutzerklärung B.7). Inhalte gelangen dabei an keine KI-App und kein KI-Modell, außer bei der Prüfung einer Fassung, die der Kunde zur Veröffentlichung im Katalog eingereicht hat. Jede Öffnung wird im Audit-Protokoll festgehalten; auf Anfrage nennt der Anbieter dem Kunden die Öffnungen seiner Bundles.

(5) Was der Kunde oder sein Agent in ein Support-Ticket oder eine Nachricht an den Anbieter schreibt, übermittelt er dem Anbieter als eigenem Verantwortlichen (Datenschutzerklärung B.9). Der Kunde nimmt darin nur auf, was für die Bearbeitung nötig ist.

(6) Für Betrieb, Sicherheit und Qualität des Dienstes, etwa um Missbrauch, Sicherheitsrisiken sowie rechtswidrige oder schädliche Inhalte zu erkennen, zur Veröffentlichung eingereichte Fassungen vorab zu prüfen und Support-Tickets einzuordnen, darf der Anbieter Inhalte als eigener Verantwortlicher automatisiert prüfen, auch mit KI-Modellen, soweit es dafür erforderlich ist (Datenschutzerklärung B.7). KI-Modelle nutzt er dafür nur bei den in Anlage 3 genannten Unterauftragsverarbeitern und nur so, dass die Daten nicht zum Training von KI-Modellen verwendet werden. Das Ergebnis einer Prüfung ist ein Hinweis: Über jede Maßnahme, die den Kunden betrifft, etwa eine Ablehnung, Sperre oder Löschung, entscheidet ein Mensch. Eine automatisierte Prüfung ist keine Öffnung im Sinne von Abs. 4; sieht sich der Anbieter daraufhin ein Bundle an, gilt Abs. 4.

§ 4 Pflichten des Anbieters

(1) Der Anbieter gewährt Zugang zu den Daten nur Personen, die zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO); nur solche Personen erhalten eine Rolle mit Zugang zu Inhalten.

(2) Der Anbieter verwendet die Daten nicht für eigene Zwecke, außer in den Fällen des § 3 Abs. 4 und 6. Er verkauft sie nicht und nutzt sie nicht zum Training von KI-Modellen.

(3) Der Anbieter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und arbeitet auf Anfrage mit der Aufsichtsbehörde zusammen.

(4) Ein Datenschutzbeauftragter ist beim Anbieter nicht zu benennen (§ 38 Abs. 1 BDSG). Ansprechpartner für den Datenschutz ist der Inhaber (Anlage 1).

§ 5 Technische und organisatorische Maßnahmen

(1) Der Anbieter trifft die Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Anbieter darf sie durch gleichwertige oder bessere ersetzen; das Schutzniveau der Anlage 2 darf nicht unterschritten werden. Wesentliche Änderungen dokumentiert er in Anlage 2. Er überprüft die Maßnahmen regelmäßig und bei jeder wesentlichen Änderung des Dienstes.

§ 6 Unterauftragsverarbeiter

(1) Der Kunde erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen (Art. 28 Abs. 2 DSGVO). Die in Anlage 3 genannten gelten als genehmigt.

(2) Der Anbieter informiert den Kunden mindestens 14 Tage, bevor er einen Unterauftragsverarbeiter hinzunimmt oder ersetzt, per E-Mail an die Adresse seines Kontos und in Anlage 3. Muss er einen Unterauftragsverarbeiter aus Gründen der Sicherheit oder weil dieser seine Leistung einstellt kurzfristig ersetzen, informiert er unverzüglich danach. Der Kunde kann der Änderung innerhalb von 14 Tagen nach der Information aus einem wichtigen datenschutzrechtlichen Grund in Textform widersprechen. Hält der Anbieter an der Änderung fest, kann jede Partei den Nutzungsvertrag fristlos kündigen; für die Zeit danach im Voraus gezahlte Entgelte werden anteilig erstattet. Im Übrigen gilt die Änderung nach Ablauf der Frist.

(3) Der Anbieter setzt Unterauftragsverarbeiter nur ein, wenn sie vertraglich Datenschutzpflichten unterliegen, die Art. 28 Abs. 4 DSGVO entsprechen (Anlage 3). Für sie haftet er wie für eigenes Handeln, im Rahmen von § 12.

(4) Keine Unterauftragsverarbeitung sind Dienste, die der Kunde selbst verbindet oder nutzt, insbesondere KI-Apps, die er an seine Bundles anschließt, sowie Leistungen eigener Verantwortlicher ohne Zugriff auf Inhalte (Anlage 3).

§ 7 Rechte der Betroffenen

(1) Korpus ermöglicht es dem Kunden, Auskunft, Berichtigung, Löschung und Datenübertragbarkeit selbst zu erfüllen: Inhalte lassen sich jederzeit lesen, ändern, exportieren und löschen.

(2) Wendet sich eine betroffene Person an den Anbieter, verweist er sie an den Kunden, soweit er diesen erkennen kann, und leitet die Anfrage unverzüglich an ihn weiter. Ohne Weisung beantwortet er sie nicht selbst.

(3) Weitergehende Unterstützung (Art. 28 Abs. 3 lit. e DSGVO) leistet der Anbieter auf Anfrage; den Aufwand vergütet der Kunde nach vorheriger Absprache, es sei denn, die Anfrage beruht auf einem Verstoß des Anbieters.

§ 8 Unterstützung und Verletzungen des Schutzes

(1) Der Anbieter unterstützt den Kunden bei den Pflichten nach Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen, zunächst durch diesen Vertrag und seine Anlagen. Weitergehende Unterstützung, etwa bei einer Datenschutz-Folgenabschätzung, leistet er auf Anfrage; den Aufwand vergütet der Kunde nach vorheriger Absprache, es sei denn, sie ist wegen eines Verstoßes des Anbieters nötig.

(2) Eine Verletzung des Schutzes personenbezogener Daten des Kunden meldet der Anbieter unverzüglich, nachdem er davon Kenntnis erlangt hat, per E-Mail an den Inhaber des Teams, in dem das betroffene Bundle liegt. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO; was noch nicht bekannt ist, reicht er nach. Er ergreift angemessene Maßnahmen zur Eindämmung. Beruht die Verletzung auf einem Verstoß des Anbieters, unterstützt er den Kunden bei dessen Meldungen nach Art. 33 und 34 DSGVO ohne Vergütung. Die Meldung ist kein Anerkenntnis eines Verschuldens.

§ 9 Ort der Verarbeitung

(1) Die Daten werden in der EU gespeichert und verarbeitet, an den in Anlage 3 genannten Orten. Nennt Anlage 3 einen Ort außerhalb des Europäischen Wirtschaftsraums, gilt Absatz 2.

(2) Verarbeitet ein Unterauftragsverarbeiter Daten in einem Drittland oder kann ein Drittland auf sie zugreifen, etwa weil er zu einem Unternehmen in den USA gehört, stützt sich die Übermittlung auf die in Anlage 3 genannten Garantien nach Art. 44 ff. DSGVO, etwa einen Angemessenheitsbeschluss oder Standardvertragsklauseln. Die Daten sind zudem bei Übertragung und Speicherung verschlüsselt (Anlage 2).

(3) Übermittlungen, die der Kunde selbst veranlasst, etwa an verbundene KI-Apps, an Personen, mit denen er teilt, oder durch einen Export, verantwortet er selbst.

§ 10 Löschung und Rückgabe

(1) Der Kunde kann seine Inhalte jederzeit selbst exportieren, mit Dateien als ein Archiv, und löschen. Der Export ist die Rückgabe im Sinne von Art. 28 Abs. 3 lit. g DSGVO.

(2) Löscht der Kunde Inhalte, ein Bundle oder sein Konto, entfernt der Anbieter die Datenbankeinträge sofort; Kopien in Sicherungen und gelöschte oder ersetzte Dateien entfallen nach den Fristen der Datenschutzerklärung (B.12), spätestens nach 35 Tagen.

(3) Endet der Nutzungsvertrag, ohne dass der Kunde sein Konto gelöscht hat, löscht der Anbieter die Inhalte des Kunden innerhalb von 30 Tagen nach dem Ende; bis dahin kann der Kunde sie exportieren. Für Dateien und Sicherungen gilt danach Absatz 2.

(4) Das Audit-Protokoll (Konto-IDs und Ereignisse, keine Inhalte) und Support-Tickets bewahrt der Anbieter nach der Datenschutzerklärung (B.8, B.9, B.12) auf. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(5) Kopien, die andere Nutzer mit Zugriff des Kunden angelegt haben, und Beiträge des Kunden in Bundles anderer Nutzer gehören zu deren Bundles und werden nach deren Vertrag behandelt.

(6) Auf Anfrage bestätigt der Anbieter die Löschung in Textform.

§ 11 Nachweise und Kontrollen

(1) Der Anbieter weist die Einhaltung seiner Pflichten nach durch diesen Vertrag und seine Anlagen, durch Auskünfte in Textform und, für die Infrastruktur, durch die öffentlich zugänglichen Zertifizierungen und Prüfberichte seiner Unterauftragsverarbeiter (bei AWS etwa ISO/IEC 27001 und BSI C5).

(2) Reicht dies im Einzelfall nicht aus, kann der Kunde selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer, der kein Wettbewerber des Anbieters ist, eine Inspektion durchführen. Sie findet zunächst aus der Ferne statt, durch Vorlage von Unterlagen und in einer Videokonferenz, vor Ort nur, wenn das nicht ausreicht. Sie wird mindestens 30 Tage vorher in Textform angekündigt, findet zu Geschäftszeiten und ohne Störung des Betriebs statt und höchstens einmal je Kalenderjahr; Ankündigungsfrist und Häufigkeit gelten nicht, wenn eine Verletzung des Schutzes der Daten des Kunden oder eine Anordnung der Aufsichtsbehörde Anlass gibt. Daten anderer Kunden und Geschäftsgeheimnisse des Anbieters sind ausgenommen. Rechenzentren der Unterauftragsverarbeiter werden nicht besichtigt; für sie gilt Absatz 1.

(3) Jede Partei trägt ihre eigenen Kosten.

(4) Kontrollen der zuständigen Aufsichtsbehörde duldet der Anbieter.

§ 12 Haftung

(1) Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 Abs. 1 bis 4 DSGVO und bleibt von diesem Vertrag unberührt.

(2) Im Verhältnis zwischen Kunde und Anbieter gelten für alle Ansprüche aus oder im Zusammenhang mit diesem Vertrag, auch für den Rückgriff nach Art. 82 Abs. 5 DSGVO, § 10 der Nutzungsbedingungen und die folgenden Absätze.

(3) Unbeschränkt haftet der Anbieter bei Vorsatz und grober Fahrlässigkeit, auch seiner gesetzlichen Vertreter und Erfüllungsgehilfen, bei der Verletzung von Leben, Körper oder Gesundheit, bei arglistig verschwiegenen Mängeln (§ 444 BGB), aus einer Garantie und nach dem Produkthaftungsgesetz.

(4) Bei leichter Fahrlässigkeit haftet der Anbieter nur für die Verletzung einer wesentlichen Vertragspflicht, also einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf, und nur für den vertragstypischen, vorhersehbaren Schaden.

(5) Ist der Kunde Unternehmer (§ 14 BGB), eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, ist die Haftung nach Absatz 4 je Schadensereignis auf den höheren der folgenden Beträge begrenzt: die Entgelte, die für Korpus in den 12 Monaten vor dem Ereignis an den Anbieter oder an den Verkäufer von Pro (§ 4 der Nutzungsbedingungen) gezahlt wurden, oder 25.000 Euro. Mehrere Verletzungen aus derselben Ursache gelten als ein Schadensereignis.

(6) Für alle Schadensereignisse eines Vertragsjahres zusammen ist die Haftung nach Absatz 5 auf den höheren der folgenden Beträge begrenzt: die Entgelte nach Absatz 5 oder 50.000 Euro. Ein Vertragsjahr umfasst zwölf Monate, das erste beginnt mit der ersten Annahme der Nutzungsbedingungen durch den Kunden.

(7) Für den Verlust von Daten haftet der Anbieter nach den Absätzen 4 bis 6 nur in Höhe des Aufwands, der zur Wiederherstellung nötig gewesen wäre, wenn der Kunde seine Inhalte in angemessenen Abständen exportiert hätte.

(8) Die Absätze 4 bis 7 gelten auch für die Haftung für Unterauftragsverarbeiter (§ 6 Abs. 3) und für die persönliche Haftung der Erfüllungsgehilfen des Anbieters. Jeder Absatz dieses Paragrafen gilt für sich; ist einer unwirksam, bleiben die anderen bestehen.

(9) Angaben in diesem Vertrag und seinen Anlagen beschreiben Leistungen und Maßnahmen; eine Garantie sind sie nur, wenn sie ausdrücklich so bezeichnet sind.

§ 13 Schlussbestimmungen

(1) Widerspricht dieser Vertrag den Nutzungsbedingungen, geht er in Fragen des Datenschutzes vor. Für die Haftung gelten ausschließlich § 10 der Nutzungsbedingungen und § 12 dieses Vertrags. Vertragsmuster oder Bedingungen des Kunden zur Auftragsverarbeitung gelten nur, wenn der Anbieter sie in Textform annimmt.

(2) Änderungen dieses Vertrags folgen § 13 der Nutzungsbedingungen: Was Rechte oder Pflichten des Kunden berührt, gilt erst, wenn er es in der App annimmt. Änderungen der Anlage 3 gelten nach § 6 Abs. 2, Änderungen der Anlage 2 nach § 5 Abs. 2 ohne Annahme.

(3) Es gilt deutsches Recht. Der Gerichtsstand richtet sich nach § 14 der Nutzungsbedingungen.

(4) Die deutsche Fassung ist verbindlich, auch wenn die Nutzungsbedingungen im Übrigen englisch sind (§ 14 der Nutzungsbedingungen). Die englische Übersetzung dient nur der Information.

(5) Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam; an ihre Stelle tritt die gesetzliche Regelung.

(6) Der Kunde kann diese Fassung jederzeit als PDF speichern. Auf Anfrage bestätigt der Anbieter in Textform, wann das Konto des Kunden diese Fassung angenommen hat, und sendet sie ihm unverändert und vom Anbieter unterschrieben.

Anlage 1: Parteien und Ansprechpartner

Auftragsverarbeiter:

Tilman Krauß
Till IT works
Bismarckstraße 17a
42799 Leichlingen
Deutschland

Datenschutz: me@till-it-works.de. Kein Datenschutzbeauftragter benannt (§ 38 Abs. 1 BDSG). Zuständige Aufsichtsbehörde: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

Verantwortlicher: der Kunde, wie in seinem Konto angegeben; Kontakt ist die E-Mail-Adresse dieses Kontos.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

- **Zutritt:** Der Anbieter betreibt keine eigenen Server. Die Rechenzentren seiner Unterauftragsverarbeiter sind nach deren Zertifizierungen physisch gesichert (bei AWS etwa ISO/IEC 27001, BSI C5).
- **Zugang:** Anmeldung über einen verwalteten Anmeldedienst (Amazon Cognito) per Passkey, Einmalcode an die E-Mail-Adresse oder, wo angeboten, einen Anmeldeanbieter, den die Person wählt. Zugriffstoken gelten höchstens 1 Stunde, Erneuerungstoken höchstens 30 Tage. Schlüssel für Programme laufen nach höchstens 1 Jahr ab, verfallen, wenn sie ungenutzt bleiben, und lassen sich jederzeit widerrufen. Von Tokens und Schlüsseln wird nur ein Hash gespeichert. Einzelheiten: Datenschutzerklärung B.4 und B.12.

- **Zugriff:** Rechte je Bundle (Lesen, Schreiben oder einzelne Pfade), bei jeder Anfrage in der Anwendung und zusätzlich in der Datenbank (Row Level Security) geprüft. Agenten erhalten nie mehr Rechte als die Person, für die sie handeln. Jeder Dienst meldet sich mit einem eigenen Datenbankbenutzer per kurzlebigem IAM-Token an, ohne gespeichertes Passwort; Anfragen der Nutzer laufen über eine Rolle, die Row Level Security nicht umgehen kann. Einsicht des Anbieters nur nach § 3 Abs. 4, lesend und protokolliert; automatisierte Prüfungen nur nach § 3 Abs. 6. Die Pipeline, die neue Versionen ausliefert, kann sich nicht an der Datenbank anmelden (ausdrückliches Verbot in ihren Rollen); Schemaänderungen führt eine eigene Funktion aus.
- **Betrieb:** Administrative Zugänge des Anbieters nur mit Mehrfaktor-Authentifizierung oder Passkey. Seine Arbeitsgeräte sind verschlüsselt, mit Bildschirmsperre und aktuellen Sicherheitsupdates.
- **Trennung:** Bundles sind in der Datenbank per Row Level Security voneinander getrennt. Produktion und Entwicklung laufen in getrennten AWS-Konten; in der Entwicklung werden keine Produktionsdaten verwendet.
- **Verschlüsselung:** Übertragung mit TLS 1.2 oder höher, auch zur Datenbank, mit Prüfung des Zertifikats. Datenbank (Amazon Aurora) und Dateien (Amazon S3) werden verschlüsselt gespeichert (AES-256, mit von AWS verwalteten Schlüsseln). Dateien sind nur über einzeln signierte Links erreichbar, die nach höchstens 15 Minuten ablaufen; öffentlicher Zugriff auf die Speicher ist gesperrt.
- **Sparsame Protokolle:** Das Audit-Protokoll führt Konto-IDs statt E-Mail-Adressen, das Änderungsprotokoll eines Bundles Konto-ID und Benutzername. Fehlerprotokolle sind so ausgelegt, dass sie keine Inhalte enthalten, und werden nach höchstens 30 Tagen gelöscht (Datenschutzerklärung B.11, B.12).

2. Integrität

- **Weitergabe:** nur verschlüsselt. Exporte liegen über einen signierten Link zum Abruf bereit, werden nach einem Tag gelöscht und entfallen danach wie gelöschte Dateien (§ 10 Abs. 2).
- **Eingabe:** Jedes Bundle führt ein Änderungsprotokoll (wer, wann, welcher Pfad, welche Änderung). Sicherheitsrelevante Ereignisse stehen im Audit-Protokoll (§ 10 Abs. 4).

3. Verfügbarkeit und Belastbarkeit

- Der Speicher der Datenbank wird über mehrere Verfügbarkeitszonen repliziert. Die Datenbank wird fortlaufend gesichert, lässt sich auf einen früheren Zeitpunkt wiederherstellen (Sicherungen höchstens 35 Tage) und ist gegen Löschung geschützt.
- Gelöschte oder ersetzte Dateien bleiben eine begrenzte Zeit wiederherstellbar (§ 10 Abs. 2).
- Die Anwendung läuft serverlos über mehrere Verfügbarkeitszonen. Eine Web Application Firewall vor der Web-App und Drosselung an allen Schnittstellen begrenzen Überlastung.

4. Regelmäßige Überprüfung

- Die Infrastruktur ist als Code beschrieben. Jede Änderung wird geprüft, automatisch getestet, auch die Zugriffsregeln, und über eine Pipeline ausgerollt.
- Die Maßnahmen werden regelmäßig und bei jeder wesentlichen Änderung des Dienstes überprüft (§ 5 Abs. 2).
- Verletzungen des Schutzes werden nach § 8 Abs. 2 gemeldet, ihre Ursache wird behoben und dokumentiert.
- Unterauftragsverarbeiter werden nur mit einem Vertrag nach Art. 28 DSGVO eingesetzt (Anlage 3).

Anlage 3: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort	Garantien
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	Cloud-Infrastruktur: Rechenleistung, Datenbank, Dateispeicher, Anmeldung, E-Mail-Versand, Auslieferung der Web-App; KI-Modelle über Amazon Bedrock (auch von Anthropic) für automatisierte Prüfungen (§ 3 Abs. 6)	EU (Frankfurt); Amazon Bedrock nur in AWS-Regionen innerhalb der EU; der Code der Web-App, keine Inhalte, auch über Edge-Standorte weltweit	AWS Data Processing Addendum; EU-US Data Privacy Framework und Standardvertragsklauseln (2021/914)
Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	KI-Modelle über die Anthropic-API für automatisierte Prüfungen (§ 3 Abs. 6); die Daten werden nicht zum Training verwendet	USA (Anthropic, PBC und deren Unterauftragsverarbeiter)	Anthropic Data Processing Addendum; Standardvertragsklauseln (2021/914)

Keine Unterauftragsverarbeiter, weil sie keine Inhalte des Kunden erhalten oder eigene Verantwortliche sind:

- Der Verkäufer von Pro (§ 4 der Nutzungsbedingungen) und sein Zahlungsdienst, als eigene Verantwortliche (Datenschutzerklärung B.5).
- Anmeldeanbieter, die eine Person selbst wählt, etwa Google oder Microsoft, als eigene Verantwortliche; sie erhalten keine Inhalte.
- Der E-Mail-Dienst des Anbieters für E-Mails an ihn, in seiner eigenen Verantwortung (Datenschutzerklärung B.14); Inhalte aus Bundles und Support-Tickets gelangen nicht dorthin.
- KI-Apps und Programme, die der Kunde selbst verbindet: Empfänger in seiner Verantwortung (§ 6 Abs. 4).