Vereinbarung über die Auftragsverarbeitung (Art. 28 DSGVO)

Anlage AV zum SAVA-Mitgliedschaftsvertrag

Fassung vom 28.10.2026

---

zwischen

dem SAVA-Mitglied, das die AGB für SAVA angenommen hat (Name und Anschrift nach den Angaben in der Bestellung) – nachfolgend „**Verantwortlicher**" oder „**Mitglied**" –

und der

Weise Verlagsberatung GmbH Kolonnenstr. 8, 10827 Berlin vertreten durch den Geschäftsführer Torsten Weise – nachfolgend „**Auftragsverarbeiter**" oder „**Anbieter**" –

– gemeinsam die „**Parteien**" –

Präambel

Der Anbieter stellt dem Mitglied im Rahmen des SAVA-Mitgliedschaftsvertrags (AGB in der jeweils gültigen Fassung) einen persönlichen Workspace auf der KI-Plattform Langdock einschließlich vorkonfigurierter KI-Assistenten („Agenten") zur Verfügung. Das Mitglied handelt dabei als Unternehmer im Sinne des § 14 BGB (AGB § 1.2) und nutzt den Workspace im Rahmen seiner Sachverständigentätigkeit. Es bringt dabei Dokumente ein, die personenbezogene Daten Dritter enthalten können (insbesondere Verfahrensakten, Schriftsätze, Angebote, Ortstermin-Unterlagen).

Für diese Daten Dritter ist das Mitglied Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Der Anbieter verarbeitet diese Daten im Auftrag des Mitglieds im Sinne von Art. 4 Nr. 8, Art. 28 DSGVO. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien für diese Auftragsverarbeitung.

Klarstellung zum Anwendungsbereich: Diese Vereinbarung erfasst ausschließlich personenbezogene Daten Dritter, die das Mitglied in den Workspace einbringt („Ebene 2").

a) **Ebene 1 – eigene Daten des Mitglieds:** Bestands-, Vertrags-, Zahlungs-, Konto- und Nutzungsdaten des Mitglieds selbst (einschließlich der E-Mail-Adresse zur Freischaltung). Insoweit ist der Anbieter Verantwortlicher (Art. 4 Nr. 7 DSGVO); es gelten die Datenschutzerklärung in ihrer jeweils aktuellen Fassung und die AGB. Diese Ebene ist nicht Gegenstand dieser Vereinbarung. Inhalte im Workspace wie Unterlagen, Eingaben, Ausgaben und Chatverläufe gehören nicht zu Ebene 1, sondern zu Ebene 2, soweit sie personenbezogene Daten Dritter enthalten.

b) **Ebene 2 – Drittdaten in eingebrachten Unterlagen:** Personenbezogene Daten Dritter, die das Mitglied in den Workspace einbringt (insbesondere aus Verfahrensakten, Schriftsätzen,

Angeboten, Ortstermin-Unterlagen), einschließlich der Eingaben, Ausgaben und Chatverläufe, die solche Daten enthalten. Insoweit ist das Mitglied Verantwortlicher und der Anbieter sein Auftragsverarbeiter. Ausschließlich diese Ebene ist Gegenstand dieser Vereinbarung.

c) **Ebene 3 – eigene Verantwortlichkeit des Anbieters:** Datenverarbeitungen, die der Anbieter außerhalb des Workspace in eigener Verantwortung vornimmt, insbesondere Website und Interessentenkommunikation, Newsletter, Buchhaltung, Support, Workshop-Teilnahmeerfassung sowie die Durchführung der Workshops und Sprechstunden einschließlich der Tonaufzeichnung und Transkription der Sprechstunden (AGB § 2.4). Insoweit ist der Anbieter Verantwortlicher; es gilt die Datenschutzerklärung. Diese Ebene ist nicht Gegenstand dieser Vereinbarung. Das Mitglied schildert in Workshops, Sprechstunden und im Support keine personenbezogenen Daten Dritter aus seinen Fällen (AGB §§ 2.4, 2.12).

---

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Verarbeitung ist die Bereitstellung und Administration eines persönlichen Workspace auf der Plattform Langdock.com einschließlich der dort bereitgestellten Agenten für die Dauer der SAVA-Mitgliedschaft.

(2) Diese Vereinbarung beginnt mit Wirksamwerden des Mitgliedschaftsvertrags und endet mit dessen Beendigung. Die Pflichten aus § 5 (Vertraulichkeit) und § 10 (Löschung) bestehen über das Vertragsende hinaus fort.

(3) Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen; sie teilt das rechtliche Schicksal des Mitgliedschaftsvertrags.

§ 2 Art und Zweck der Verarbeitung

(1) Die Verarbeitung umfasst das Hosting, die Speicherung und die KI-gestützte Verarbeitung der vom Mitglied eingebrachten Inhalte sowie die technische Administration des Workspace (Anlegen, Sperren und Löschen von Konten, Lizenzzuweisung, Modell-Freischaltung, Vollzug der Löschung nach § 10).

(2) Eine inhaltliche Kenntnisnahme der vom Mitglied eingebrachten Inhalte durch den Anbieter findet nicht statt. Der Anbieter verzichtet auf jede Einsichtnahme in Inhalte des Mitglieds über Administrations-, Governance-, Analyse- oder vergleichbare Funktionen der Plattform und hält solche Funktionen deaktiviert, soweit die Plattform dies zulässt. Ausgenommen sind a) Einsichtnahmen, soweit eine gesetzliche Pflicht oder eine vollziehbare behördliche oder gerichtliche Anordnung dies erfordert, beschränkt auf das zwingend Erforderliche, dokumentiert und mit unverzüglicher Benachrichtigung des Mitglieds, soweit dies zulässig ist, b) Einsichtnahmen auf ausdrückliche Einzelweisung des Mitglieds in Textform im Rahmen des Supports, beschränkt auf das Erforderliche und dokumentiert, c) rein technische Verwaltungshandlungen ohne inhaltliche Kenntnisnahme und d) aggregierte,

nicht auf einzelne Mitglieder oder Inhalte beziehbare Nutzungsstatistiken. Eine Änderung von § 6.3 der AGB schränkt diesen Verzicht nicht ein.

§ 3 Datenkategorien, betroffene Personen, Pflichten des Mitglieds

(1) **Datenkategorien:** Vom Mitglied eingebrachte Inhaltsdaten, insbesondere aus Verfahrensakten, Schriftsätzen, Angeboten, Fotos und Ortstermin-Unterlagen; darin enthaltene personenbezogene Daten Dritter (Stammdaten, Kommunikationsdaten, Vertrags- und Schadensdaten). Besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO und Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO sind von der Verarbeitung ausgeschlossen (Absatz 3).

(2) **Betroffene Personen:** Verfahrensbeteiligte (Parteien, Zeugen, Bevollmächtigte), Auftraggeber, Handwerker, Sachbearbeiter von Versicherungen sowie sonstige in den Unterlagen genannte Dritte.

(3) **Schwärzungs- und Pseudonymisierungspflicht:** Das Mitglied bringt keine Daten nach Art. 9 Abs. 1 und Art. 10 DSGVO in den Workspace ein. Enthalten Unterlagen solche Daten, schwärzt oder pseudonymisiert das Mitglied sie vor dem Einbringen so, dass ein Personenbezug ohne Hinzuziehung zusätzlicher Informationen nicht hergestellt werden kann. Im Übrigen prüft das Mitglied vor dem Einbringen, ob personenbezogene Daten Dritter für den Verarbeitungszweck erforderlich sind, und schwärzt oder pseudonymisiert nicht erforderliche Angaben, soweit der Auftrag dies zulässt.

(4) Das Mitglied bleibt für die Rechtmäßigkeit der Verarbeitung, insbesondere für die Rechtsgrundlage und die Erfüllung der Informationspflichten nach Art. 13/14 DSGVO gegenüber den Betroffenen, allein verantwortlich.

§ 4 Weisungsrecht des Verantwortlichen

(1) Der Anbieter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Mitglieds, sofern er nicht durch Unionsrecht oder das Recht eines Mitgliedstaats zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Anbieter dem Mitglied diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

(2) Die Nutzung der Plattformfunktionen durch das Mitglied (insbesondere Hochladen von Unterlagen, Eingaben an Agenten, Anlegen eigener Agenten, Löschvorgänge) gilt als dokumentierte Weisung. Darüber hinausgehende Einzelweisungen bedürfen der Textform und werden von beiden Parteien dokumentiert.

(3) Der Anbieter leitet Weisungen, soweit erforderlich, über den zwischen ihm und der Langdock GmbH bestehenden Auftragsverarbeitungsvertrag an den Unterauftragsverarbeiter weiter.

(4) Hält der Anbieter eine Weisung für rechtswidrig, informiert er das Mitglied unverzüglich und ist berechtigt, die Ausführung auszusetzen, bis die Weisung bestätigt oder geändert wird. Eine Pflicht zur rechtlichen Prüfung von Weisungen besteht nicht.

§ 5 Vertraulichkeit und zur Verarbeitung befugte Personen

(1) Der Anbieter gewährleistet, dass sich alle zur Verarbeitung der Daten befugten Personen schriftlich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Befugt sind derzeit der Geschäftsführer des Anbieters sowie ein externer Auftragnehmer, der gemäß Satz 1 schriftlich zur Vertraulichkeit verpflichtet ist und den Anbieter bei Support- und Administrationsaufgaben sowie im Vertretungsfall unterstützt. Werden weitere Personen (Mitarbeiter, freie Auftragnehmer) einbezogen, gilt Satz 1 vor Aufnahme ihrer Tätigkeit.

(2) Die Vertraulichkeitspflicht besteht nach Beendigung dieser Vereinbarung fort. Ergänzend gilt § 7 der AGB (Vertraulichkeit); bei Widersprüchen geht für Daten der Ebene 2 diese Vereinbarung vor.

(3) Für fremde Geheimnisse, die dem Anbieter bei seiner Tätigkeit für das Mitglied bekannt werden, gilt ergänzend die Verpflichtung zur Verschwiegenheit nach § 203 StGB (Anlage V der AGB). Der Anbieter verpflichtet die in Absatz 1 genannten Personen auch nach § 203 StGB und belehrt sie über die Strafbarkeit.

§ 6 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Anbieter trifft die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen und passt sie dem Stand der Technik an. Eine Fortschreibung ist zulässig, sofern das Schutzniveau nicht unterschritten wird; wesentliche Änderungen teilt der Anbieter dem Mitglied mit.

(2) Soweit Maßnahmen in der Sphäre des Unterauftragsverarbeiters liegen (Hosting, Verschlüsselung, Zertifizierungen), verweist Anlage 1 auf dessen dokumentierte Angaben mit Stand-Datum (Langdock Trust Center, Beweisordner „TOM Governance").

§ 7 Unterauftragsverarbeiter

(1) Das Mitglied erteilt die allgemeine Genehmigung zur Einschaltung der in Anlage 2 aufgeführten Unterauftragsverarbeiter. Derzeit sind dies die Langdock GmbH, Greifswalder Straße 212, 10405 Berlin (Plattformbetrieb und Hosting), und der externe Auftragnehmer nach § 5 Abs. 1 (Support, Administration und Vertretung). Die Genehmigung umfasst die von der Langdock GmbH eingesetzten weiteren Unterauftragsverarbeiter, insbesondere die Anbieter der freigeschalteten KI-Modelle, nach deren jeweils aktueller Liste (Anlage 2).

(2) Der Anbieter hat mit jedem Unterauftragsverarbeiter einen Vertrag geschlossen, der diesem dieselben Datenschutzpflichten auferlegt, wie sie in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO).

(3) Der Anbieter informiert das Mitglied vorab in Textform über jede beabsichtigte Aufnahme oder Ersetzung eines Unterauftragsverarbeiters. Das Mitglied kann der Änderung innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, steht beiden Parteien ein Sonderkündigungsrecht für den Mitgliedschaftsvertrag zum Zeitpunkt des Wirksamwerdens der Änderung zu. Über Änderungen bei den weiteren Unterauftragsverarbeitern der Langdock GmbH informiert der Anbieter, sobald er davon Kenntnis erhält.

(4) Drittländer: Für den SAVA-Workspace sind ausschließlich KI-Modelle freigeschaltet, deren Verarbeitung innerhalb der EU erfolgt; die Daten werden in Deutschland gespeichert. Soweit Unterauftragsverarbeiter der Langdock GmbH ihren Sitz in den USA haben (derzeit Sentry und Cloudflare), sind mögliche Übermittlungen durch das EU-US Data Privacy Framework und Standardvertragsklauseln abgesichert. Sollte der Anbieter künftig Modelle mit Verarbeitung außerhalb der EU freischalten wollen, gilt dies als Änderung im Sinne des Absatzes 3; die Übermittlung würde auf die Standardvertragsklauseln der EU-Kommission und – soweit einschlägig – eine Zertifizierung nach dem EU-US Data Privacy Framework gestützt. Der Anbieter schaltet nur Modelle frei, bei denen nach den Nutzungsbedingungen der Langdock GmbH (Anlage 1, Version 2.1) keine Speicherung von Prompts und Ausgaben zur Missbrauchsüberwachung und keine Überprüfung durch Menschen erfolgt; ausgenommen ist nach Angaben von Langdock die automatisierte Prüfung von Bild- und Dateieingaben bei OpenAI auf Darstellungen sexuellen Kindesmissbrauchs mit manueller Prüfung nur im Trefferfall. Er dokumentiert diese Angaben mit Stand-Datum.

§ 8 Unterstützung bei Betroffenenrechten

(1) Der Anbieter unterstützt das Mitglied mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Art. 12–22 DSGVO zu beantworten, soweit das Mitglied hierzu auf die im Workspace gespeicherten Daten nicht selbst zugreifen kann.

(2) Wendet sich eine betroffene Person unmittelbar an den Anbieter, leitet dieser das Ersuchen unverzüglich an das Mitglied weiter und beantwortet es nicht selbst, es sei denn, er ist hierzu gesetzlich verpflichtet.

(3) Praktischer Regelfall: Das Mitglied verfügt über vollständigen Zugriff auf seinen Workspace und kann Auskunft, Berichtigung und Löschung selbst vollziehen; die Unterstützungspflicht des Anbieters greift subsidiär.

§ 9 Meldepflichten und weitere Unterstützungspflichten

(1) Der Anbieter meldet dem Mitglied jede Verletzung des Schutzes personenbezogener Daten, die Daten der Ebene 2 betrifft, unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntniserlangung, in Textform an die vom Mitglied hinterlegte E-Mail-Adresse. Die Meldung enthält die Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar; Informationen können schrittweise nachgereicht werden. Dies gilt auch für Vorfälle, bei denen fremde

Geheimnisse unbefugt offenbart worden sein können. Der Anbieter unterhält hierfür einen dokumentierten Ablauf.

(2) Der Anbieter unterstützt das Mitglied bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit der Verarbeitung, Meldung an die Aufsichtsbehörde, Benachrichtigung Betroffener, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Er stellt dem Mitglied eine Muster-Datenschutz-Folgenabschätzung für den Einsatz von SAVA zur Verfügung und aktualisiert sie bei wesentlichen Änderungen.

§ 10 Löschung und Rückgabe

(1) Das Mitglied kann seine Inhalte während der Vertragslaufzeit selbst sichern: Chatverläufe lassen sich einzeln exportieren oder kopieren, hochgeladene Dateien liegen dem Mitglied im Original vor. Auf Weisung in Textform unterstützt der Anbieter die Rückgabe im Rahmen der technischen Möglichkeiten der Plattform. Nach Vertragsende werden die Daten nach § 2.7 der AGB gelöscht.

(2) Nach Ablauf der Frist nach § 2.7 der AGB löscht der Anbieter sämtliche Daten der Ebene 2, sofern nicht Unionsrecht oder das Recht eines Mitgliedstaats eine Aufbewahrung vorschreibt. Die Löschung umfasst die Daten beim Unterauftragsverarbeiter einschließlich der Sicherungskopien, die nach dessen Sicherungszyklus überschrieben werden.

(3) Auf Verlangen bestätigt der Anbieter die Löschung in Textform.

§ 11 Nachweise und Kontrollen

(1) Der Anbieter stellt dem Mitglied alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung. Hierzu gehören insbesondere aktuelle Zertifikate und Prüfberichte der Langdock GmbH mit Stand-Datum.

(2) Weitergehende Inspektionen vor Ort sind nach vorheriger Ankündigung mit angemessener Frist während der üblichen Geschäftszeiten möglich; der Anbieter kann sie von der Unterzeichnung einer Vertraulichkeitsvereinbarung abhängig machen und für den Aufwand eine angemessene Vergütung verlangen, soweit die Inspektion nicht durch einen konkreten, dokumentierten Anlass veranlasst ist.

(3) Für Kontrollen beim Unterauftragsverarbeiter gelten die Nachweis- und Auditrechte aus dem Vertrag zwischen Anbieter und Unterauftragsverarbeiter; der Anbieter macht diese auf Verlangen des Mitglieds geltend.

§ 12 Haftung und Freistellung

(1) Für die Haftung der Parteien untereinander gilt § 4 der AGB (einschließlich der Haftungsobergrenze nach § 4.2a und der Regelung zu Drittanbieter-Output nach § 4.9) auch für Ansprüche im Zusammenhang mit dieser Vereinbarung.

(2) Im Innenverhältnis der Parteien gilt für Ansprüche Dritter nach Art. 82 DSGVO die Verantwortungsverteilung des Art. 82 Abs. 2 und 3 DSGVO; § 4 der AGB bleibt im Übrigen unberührt.

(3) Das Mitglied stellt den Anbieter von Ansprüchen Dritter frei, die darauf beruhen, dass das Mitglied Daten ohne ausreichende Rechtsgrundlage eingebracht oder seine Pflichten aus § 3 verletzt hat, es sei denn, das Mitglied hat die Pflichtverletzung nicht zu vertreten.

§ 13 Schlussbestimmungen

(1) Diese Vereinbarung wird als Anlage Bestandteil des SAVA-Mitgliedschaftsvertrags. Neumitglieder bestätigen sie im Buchungsprozess, Bestandsmitglieder durch Zustimmung in Textform. Die Zustimmung wird dokumentiert.

(2) Änderungen und Ergänzungen bedürfen der Textform (im Gleichlauf mit AGB § 9.4).

(3) Bei Widersprüchen zwischen dieser Vereinbarung und den AGB geht für die Verarbeitung von Daten der Ebene 2 diese Vereinbarung vor.

(4) Die Einrede des Zurückbehaltungsrechts ist hinsichtlich der verarbeiteten Daten ausgeschlossen.

(5) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der Vereinbarung im Übrigen unberührt.

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

Stand 28.10.2026. Gliederung nach Art. 32 Abs. 1 DSGVO. Angaben des Unterauftragsverarbeiters jeweils mit Quelle und Stand-Datum.

1. Zutritts-, Zugangs- und Zugriffskontrolle (Vertraulichkeit)

- Zutrittskontrolle zu den Rechenzentren nach Angaben des Unterauftragsverarbeiters: Hosting in zertifizierten Rechenzentren von Microsoft Azure in Frankfurt mit redundanter Infrastruktur (Langdock Nutzungsbedingungen und DPA, jeweils Version 2.1, Anlage 3, Stand 26.10.2026).
- Persönliche, nicht übertragbare Zugänge je Mitglied (AGB § 2.5); Anlage der Konten ausschließlich durch den Anbieter (AGB § 2.10).
- Anmeldung über die hinterlegte E-Mail-Adresse; Langdock bietet keine eigene Zwei-Faktor-Authentifizierung (Langdock-Dokumentation, Stand 28.10.2026). Der Schutz des Kontos hängt deshalb am E-Mail-Postfach: Für die Administratorkonten von Geschäftsführer und externem Auftragnehmer ist die Zwei-Faktor-Authentifizierung des E-Mail-Postfachs Pflicht, den Mitgliedern wird sie empfohlen (Nutzungshinweise).
- Mandantentrennung: privater Workspace-Bereich je Mitglied; Inhalte für andere Mitglieder nur nach ausdrücklicher Freigabe durch das Mitglied sichtbar (AGB § 6.2).

- Inhalte des privaten Bereichs sind für andere Mitglieder nur sichtbar, wenn das Mitglied sie ausdrücklich freigibt (AGB § 6.2). Eine technische Sperre der Freigabe in den öffentlichen Bereich bietet die Plattform nicht. Inhalte mit Fallbezug dürfen dort nicht geteilt werden (AGB § 2.13 Abs. 4); Verstöße berechtigen zur Sperrung nach AGB § 2.13 Abs. 6.
- Administrative Einsichtsfunktionen („Governance"-Add-on u. a.) deaktiviert und Option „Private Agenten aus der Compliance-Ansicht ausblenden" aktiviert (dokumentiert in Screenshot mit Datum); vertraglicher Verzicht nach AGB § 6.3 Abs. 2
- Zulässig bleiben ausschließlich die Ausnahmen nach § 2 Abs. 2 dieser Vereinbarung, insbesondere technische Verwaltungshandlungen ohne inhaltliche Kenntnisnahme und aggregierte, nicht personenbeziehbare Statistiken.
- Berechtigungskonzept: Administratorrechte ausschließlich für den Geschäftsführer und den externen Auftragnehmer, jede Einsichtnahme nach § 2 Abs. 2 wird dokumentiert.

2. Modell- und Datenflusssteuerung

- Freischaltung ausschließlich EU-verarbeitender KI-Modelle durch den Anbieter als Workspace-Administrator (Screenshot Modell-Freischaltung)
- Kein Training der KI-Modelle mit Mitgliedsdaten nach Angaben des Unterauftragsverarbeiters (Langdock Nutzungsbedingungen Version 2.1, Anlage 1; Trust Center, Stand 26.10.2026).
- Keine Speicherung zur Missbrauchsüberwachung und keine Überprüfung durch Menschen bei den Modellanbietern nach den Nutzungsbedingungen der Langdock GmbH (Version 2.1, Anlage 1), mit der Ausnahme nach § 7 Abs. 4; Verarbeitung in der EU, US-Unterauftragsverarbeiter von Langdock abgesichert nach § 7 Abs. 4.
- Websuche und Integrationen mit Drittdiensten nur für Agenten aktiviert, die sie benötigen, ohne Übergabe von Fallinhalten.

3. Übertragungs-, Speicher- und Eingabekontrolle (Integrität)

- Transportverschlüsselung (mindestens TLS 1.2) sowie Verschlüsselung ruhender Daten und der Sicherungskopien (mindestens AES-256) nach Angaben des Unterauftragsverarbeiters (Langdock DPA Version 2.1, Anlage 3, Stand 26.10.2026).
- Hosting in Deutschland (Microsoft Azure, Frankfurt) nach Angaben des Unterauftragsverarbeiters; Langdock ist nach ISO 27001:2022 zertifiziert und nach SOC 2 Type II geprüft (Trust Center, Stand 26.10.2026).
- Keine Übermittlung von Unterlagen mit Daten Dritter über E-Mail, Support oder sonstige Kanäle außerhalb des Workspace (AGB §§ 2.6, 2.12).
- Protokollierung administrativer Handlungen, soweit die Plattform dies ermöglicht.

4. Verfügbarkeit, Wiederherstellbarkeit und Löschung

- Backup- und Wiederherstellungskonzept, verschlüsselte Sicherungskopien, Überwachung der Sicherungen und regelmäßige Wiederherstellungstests nach Angaben des Unterauftragsverarbeiters (Langdock DPA Version 2.1, Anlage 3). Sicherungsintervall und Aufbewahrungsdauer der Sicherungskopien nennt Langdock nicht öffentlich.
- Verfügbarkeit nach AGB § 2.14, Information der Mitglieder bei länger andauernden Störungen.
- Löschkonzept: Löschung sämtlicher Workspace-Daten nach Ablauf der Fristen nach AGB § 2.7 einschließlich der Sicherungskopien beim Unterauftragsverarbeiter, vorbehaltlich gesetzlicher Aufbewahrungspflichten (§ 10 dieser Vereinbarung), Vollzug durch den Anbieter, Bestätigung auf Verlangen.
- Sicherung der Inhalte durch das Mitglied während der Laufzeit nach § 10 Abs. 1.

5. Pseudonymisierung und Datenminimierung

- Ausschluss von Daten nach Art. 9 und 10 DSGVO, Schwärzungs- und Pseudonymisierungspflicht des Mitglieds (§ 3 Abs. 3).
- Geplant, ohne Zusage: Hinweis auf Schwärzung und Pseudonymisierung beim Hochladen, Agent zur Pseudonymisierung von Unterlagen, Verfallsfristen für Chats und Uploads als Voreinstellung.

6. Organisationskontrolle und regelmäßige Überprüfung

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 1 und 2 DSGVO) geführt; maßgeblich ist die jeweils aktuelle Fassung mit dokumentierter Änderungshistorie.
- Beweisordner „TOM Governance" mit datierten Nachweisen; Überprüfung der Anlage 1 mindestens jährlich sowie bei relevanten Plattformänderungen (AGB § 2.8).
- Zur Verarbeitung befugte Personen: der Geschäftsführer sowie ein nach § 5 Abs. 1 schriftlich zur Vertraulichkeit verpflichteter externer Auftragnehmer (Support/Vertretung; namentlich dokumentiert im VVT V11); Erweiterungen nur nach § 5 Abs. 1.
- Verpflichtung des Geschäftsführers und des externen Auftragnehmers auf Vertraulichkeit und nach § 203 StGB, Schulungen zu Datenschutz und KI-Kompetenz mit Nachweis.
- Eigene Infrastruktur des Anbieters: verschlüsselte und aktuelle Endgeräte, Bildschirmsperre, Passwortmanager, Zwei-Faktor-Authentifizierung für alle Dienste.
- Dokumentierter Ablauf für Datenschutz- und Sicherheitsvorfälle mit Meldung an die Mitglieder binnen 48 Stunden (§ 9 Abs. 1).

Anlage 2: Genehmigte Unterauftragsverarbeiter

Unternehmen	Anschrift	Leistung	Vertragsgrundlage
Langdock GmbH	Greifswalder Straße 212, 10405 Berlin, Deutschland	Betrieb der KI-Plattform, Hosting des Workspace, Bereitstellung der KI-Modelle (nur EU-Verarbeitung, § 7 Abs. 4)	AVV Anbieter↔Langdock: DPA Version 2.1, einbezogen über die Nutzungsbedingungen (bestätigt durch Langdock-Support 02/2026); Zusatzvereinbarung für Berufsgeheimnisträger vom 06.10.2026
Andreas Buchhalter, spielbar digital	Unterstr. 134c, 53859 Niederkassel	Support, Administration und Vertretung, Einsicht in Inhalte nur nach § 2 Abs. 2	Vertrag nach Art. 28 Abs. 4 DSGVO, Verpflichtung nach § 203 StGB

Die Langdock GmbH setzt weitere Unterauftragsverarbeiter ein (Anlage 2 des Langdock-DPA, Version 2.1, und trust.langdock.com/subprocessors, Stand 26.10.2026): Microsoft Ireland Operations Ltd. (Hosting und KI-Modelle, EU), Amazon Web Services EMEA SARL (KI-Modelle, EU), Google Cloud EMEA Ltd. (KI-Modelle, EU), OpenAI Ireland Ltd. (KI-Modelle, EU), Mistral AI SAS (KI-Modelle, EU), Functional Software Inc. – Sentry, USA (Fehlerdiagnose, Verarbeitung in der EU), Cloudflare Inc., USA (Schutz vor schädlichem Datenverkehr, Verarbeitung in der EU). Maßgeblich ist die jeweils aktuelle Liste; Änderungen veröffentlicht Langdock 14 Tage vorher. Freigeschaltet sind nur Modelle mit Verarbeitung in der EU (§ 7 Abs. 4).

Nicht in dieser Anlage enthalten sind Dienstleister der Ebene 1/3 (u. a. Ablefy, Proton, Quentn, Jamie/wespond, GetMyInvoices, IONOS): Sie sind für die Verarbeitung von Ebene-2-Daten nicht vorgesehen und sind Auftragsverarbeiter des Anbieters in dessen eigener Verantwortlichkeit, siehe DSE und VVT Teil B. Das Mitglied bringt Unterlagen mit personenbezogenen Daten Dritter ausschließlich über den Workspace ein und übermittelt sie nicht über Support- oder sonstige Kommunikationskanäle (insbesondere nicht per E-Mail); § 3 Abs. 3 gilt entsprechend.