Auftragsverarbeitungsvereinbarung (AVV)
gemäß Art. 28 Abs. 3 DSGVO für die kostenlose Rechnungsdiagnostik

Version 1.0 – Stand: 31.07.2026

zwischen

dem Unternehmen, das die Diagnostik anfordert, vertreten durch die Person, die diese Vereinbarung im Rahmen der Registrierung annimmt (nachfolgend „**Verantwortlicher**"),

und

Emblon, Inhaber: Konstantin Arndt, Cranachstr. 38, 40235 Düsseldorf (nachfolgend „**Auftragsverarbeiter**" oder „**Emblon**").

Präambel

Der Verantwortliche nimmt eine kostenlose, einmalige Diagnostik in Anspruch, bei der Emblon eingereichte Eingangsrechnungen und zugehörige Nachweise (z. B. Leistungsnachweise, Stundennachweise, Zertifikate) anhand eines regelbasierten Prüfrasters mit KI-gestützter Datenextraktion auswertet und dem Verantwortlichen einen Diagnosebericht übermittelt. Dabei verarbeitet Emblon personenbezogene Daten im Auftrag des Verantwortlichen. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO. Sie ist bewusst auf diesen engen, zeitlich begrenzten Anwendungsfall zugeschnitten.

---

§ 1 Abschluss, Gegenstand und Dauer

(1) Diese Vereinbarung wird in einem elektronischen Format im Sinne des Art. 28 Abs. 9 DSGVO geschlossen. Der Abschluss erfolgt, indem eine für den Verantwortlichen handelnde Person im Registrierungsformular das entsprechende Kontrollkästchen aktiviert und die angegebene geschäftliche E-Mail-Adresse anschließend über den zugesandten Bestätigungslink verifiziert. Emblon zeichnet Version und Datum der angenommenen Vereinbarung, den Zeitstempel der Annahme und der Verifizierung sowie die annehmende E-Mail-Adresse und den angegebenen Unternehmensnamen auf und hält diese Aufzeichnung zu Nachweiszwecken vor.

(2) Die annehmende Person erklärt mit der Annahme, zum Abschluss dieser Vereinbarung für den Verantwortlichen berechtigt zu sein. Der Verantwortliche muss sich das Handeln von Personen, die unter einer geschäftlichen E-Mail-Adresse seiner Domain auftreten, nach den Grundsätzen der Anscheins- und Duldungsvollmacht zurechnen lassen.

(3) Gegenstand der Vereinbarung ist ausschließlich die in Anlage 1 beschriebene Verarbeitung zur Durchführung der einmaligen, kostenlosen Diagnostik. Für andere oder künftige Leistungen gilt diese Vereinbarung nicht; hierfür wäre eine gesonderte Vereinbarung zu schließen.

(4) Die Vereinbarung beginnt mit der Annahme nach Absatz 1 und endet automatisch mit der vollständigen Löschung der Quelldaten nach § 10. Einer Kündigung bedarf es nicht. Der Verantwortliche kann die Verarbeitung jederzeit ohne Angabe von Gründen beenden; in diesem Fall gilt § 10 Abs. 3.

§ 2 Beschreibung der Verarbeitung

Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen sind in **Anlage 1** festgelegt. Die Verarbeitung findet ausschließlich in Rechenzentren innerhalb der EU bzw. des EWR statt (§ 7).

§ 3 Weisungen des Verantwortlichen

(1) Emblon verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, Emblon ist nach dem Recht der Union oder eines Mitgliedstaats hierzu verpflichtet; in einem solchen Fall teilt Emblon dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Als dokumentierte Erstweisung gelten diese Vereinbarung einschließlich ihrer Anlagen sowie die Übermittlung der Dokumente durch den Verantwortlichen im dafür vorgesehenen Einreichungsverfahren. Weitere Einzelweisungen (insbesondere zur vorzeitigen Löschung) erteilt der Verantwortliche in Textform von der verifizierten E-Mail-Adresse an **datenschutz@emblon.de**.

(3) Hält Emblon eine Weisung für einen Verstoß gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten, informiert Emblon den Verantwortlichen unverzüglich. Emblon ist berechtigt, die Ausführung der betreffenden Weisung bis zu einer Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

§ 4 Vertraulichkeit

Emblon gewährleistet, dass sich alle zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht über die Beendigung dieser Vereinbarung hinaus fort. Der Zugriff ist auf die Personen beschränkt, die ihn zur Durchführung der Diagnostik benötigen.

§ 5 Sicherheit der Verarbeitung

(1) Emblon trifft alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Abschlusses implementierten Maßnahmen sind in **Anlage 2** beschrieben; sie sind für die konkrete Verarbeitung (kleine Datenmengen, kurze Speicherdauer, geschlossener Empfängerkreis) angemessen im Sinne des risikobasierten Ansatzes der DSGVO.

(2) Emblon darf die Maßnahmen an den Stand der Technik anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zur Einschaltung der in **Anlage 3** aufgeführten Unterauftragsverarbeiter.

(2) Emblon informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 14 Tage vor deren Wirksamwerden in Textform an die verifizierte E-Mail-Adresse. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus datenschutzrechtlichen Gründen widersprechen. Im Fall des Widerspruchs kann jede Partei die Verarbeitung beenden; die eingereichten Daten werden dann nach § 10 gelöscht. Angesichts der kurzen Laufzeit der Diagnostik ist mit Änderungen während einer laufenden Verarbeitung nicht zu rechnen.

(3) Emblon erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet Emblon gegenüber dem Verantwortlichen für die Einhaltung von dessen Pflichten.

(4) Nicht als Unterauftragsverarbeitung gelten Leistungen Dritter ohne Zugriff auf personenbezogene Daten des Verantwortlichen (z. B. Telekommunikationsleistungen, Wartung ohne Datenzugriff).

§ 7 Verarbeitungsort; keine Drittlandübermittlung

(1) Emblon verarbeitet und speichert die personenbezogenen Daten des Verantwortlichen ausschließlich in Rechenzentren innerhalb der EU bzw. des EWR. Auch die KI-gestützte Datenextraktion erfolgt ausschließlich über Sprachmodelle (LLM), die innerhalb der Plattform Azure AI Foundry in der EU-/EWR-Infrastruktur von Microsoft betrieben werden und deren Verarbeitung vertraglich und technisch auf EU-/EWR-Rechenzentren beschränkt ist (Anlage 3). Emblon ist berechtigt, die eingesetzten Modelle zu wechseln oder mehrere Modelle parallel einzusetzen, sofern diese von Microsoft innerhalb der EU bzw. des EWR bereitgestellt werden und den Bestimmungen dieser Vereinbarung, insbesondere § 14 (kein Training) und diesem § 7 (EU-Verarbeitung), unterliegen.

(2) Eine Übermittlung in Drittländer ist weder beabsichtigt noch für die Diagnostik erforderlich. Sollte eine solche Übermittlung ausnahmsweise aufgrund zwingenden Rechts erforderlich werden, erfolgt sie nur unter Einhaltung der Voraussetzungen des Kapitels V der DSGVO (insbesondere Art. 44 ff. DSGVO) und nach vorheriger Information des Verantwortlichen gemäß § 3 Abs. 1.

(3) Die in Anlage 3 genannten Unterauftragsverarbeiter sind mit ihren vertragschließenden Gesellschaften in der EU ansässig. Soweit sie Konzernen mit Sitz außerhalb der EU angehören, bestehen vertragliche Zusagen zur Datenlokalisierung in der EU (u. a. Microsoft EU Data Boundary) sowie – als zusätzliche Absicherung für den nicht beabsichtigten Ausnahmefall – Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO.

§ 8 Rechte betroffener Personen

(1) Emblon unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen (Art. 12–23 DSGVO) nachzukommen. Angesichts der kurzen Speicherdauer betrifft dies vor allem Auskunft und Löschung; einer Löschweisung kommt Emblon unverzüglich, spätestens innerhalb von 5 Werktagen nach.

(2) Wendet sich eine betroffene Person unmittelbar an Emblon, leitet Emblon den Antrag unverzüglich an den Verantwortlichen weiter und beantwortet ihn nicht selbst, es sei denn, der Verantwortliche weist Emblon hierzu an oder Emblon ist gesetzlich zur Antwort verpflichtet.

§ 9 Unterstützungspflichten; Meldung von Verletzungen

(1) Emblon unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der Emblon zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen an die Aufsichtsbehörde, Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(2) Emblon meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betrifft, unverzüglich nach Bekanntwerden, spätestens innerhalb von 48 Stunden, an die verifizierte E-Mail-Adresse. Die Meldung enthält, soweit bereits bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO (Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Abhilfemaßnahmen); nicht sofort verfügbare Informationen werden ohne unangemessene Verzögerung nachgereicht. Emblon dokumentiert Verletzungen einschließlich der Abhilfemaßnahmen.

(3) Die Bewertung der Meldepflicht gegenüber Aufsichtsbehörden und betroffenen Personen sowie die Meldung selbst obliegen dem Verantwortlichen.

§ 10 Löschung und Rückgabe

(1) Emblon löscht sämtliche Quelldaten – eingereichte Dokumente, per E-Mail weitergeleitete Ursprungsnachrichten samt Anhängen sowie hieraus extrahierte personenbezogene Inhalte – **spätestens 30 Tage nach Zustellung des Diagnoseberichts.** Die Löschung erfolgt aus allen

Produktivsystemen; Kopien in Sicherungssystemen werden **spätestens 35 Tage** danach durch turnusmäßiges Überschreiben bzw. Ablauf der Sicherungszyklen beseitigt und sind bis dahin gegen jede anderweitige Nutzung gesperrt.

(2) Eine Rückgabe der Daten ist nicht erforderlich, da der Verantwortliche die Originale behält; auf Wunsch bestätigt Emblon die Löschung in Textform.

(3) Auf Weisung des Verantwortlichen löscht Emblon die Quelldaten jederzeit vorzeitig, unverzüglich, spätestens innerhalb von 5 Werktagen.

(4) Von der Löschpflicht ausgenommen sind ausschließlich (a) Daten, deren Aufbewahrung Emblon nach Unionsrecht oder dem Recht eines Mitgliedstaats obliegt, sowie (b) anonymisierte Leistungsdaten nach § 14, die keinen Personenbezug mehr aufweisen und daher nicht der DSGVO unterliegen. Die Aufzeichnung des Vertragsschlusses nach § 1 Abs. 1 bewahrt Emblon als eigener Verantwortlicher zu Nachweiszwecken auf (siehe Datenschutzerklärung).

§ 11 Nachweise; Kontrollrechte

(1) Emblon stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind, insbesondere die Beschreibung der technischen und organisatorischen Maßnahmen (Anlage 2), Löschprotokolle sowie einschlägige Zertifizierungen und Prüfberichte der eingesetzten Infrastruktur (u. a. ISO/IEC 27001, SOC 2 der Microsoft-Azure-Plattform).

§ 12 Garantien des Verantwortlichen; Daten Dritter

(1) Die eingereichten Dokumente enthalten regelmäßig personenbezogene Daten Dritter, insbesondere von Ansprechpartnern, Inhabern und Beschäftigten der Lieferanten des Verantwortlichen (z. B. Namen, dienstliche Kontaktdaten, IBAN, in Stundennachweisen ggf. Tätigkeits- und Zeitangaben). Diese Personen stehen in keiner Beziehung zu Emblon; allein der Verantwortliche entscheidet, welche Dokumente er einreicht.

(2) Der Verantwortliche garantiert im Sinne einer selbstständigen, verschuldensunabhängigen Einstandspflicht, dass

a) für die Offenlegung der eingereichten Dokumente an Emblon und deren Verarbeitung im Rahmen der Diagnostik eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO besteht (regelmäßig Art. 6 Abs. 1 lit. f DSGVO – berechtigtes Interesse an der Prüfung von Eingangsrechnungen im Rahmen ordnungsgemäßer Buchführung und Rechnungsprüfung);

b) er die ihm gegenüber den betroffenen Personen obliegenden Informationspflichten (Art. 13, 14 DSGVO) erfüllt hat oder sich auf eine Ausnahme, insbesondere Art. 14 Abs. 5 DSGVO, stützen kann; und

c) der Einreichung keine vertraglichen oder gesetzlichen Verschwiegenheitspflichten entgegenstehen.

(3) Der Verantwortliche stellt Emblon von allen Ansprüchen Dritter – einschließlich Ansprüchen betroffener Personen nach Art. 82 DSGVO – sowie von Bußgeldern und behördlichen Maßnahmen frei, soweit diese auf einer Verletzung der Garantien nach Absatz 2 oder auf einer rechtswidrigen Weisung des Verantwortlichen beruhen. Die Freistellung umfasst die Kosten angemessener Rechtsverteidigung. Sie gilt nicht, soweit Emblon der Verstoß bekannt war oder infolge grober Fahrlässigkeit unbekannt blieb.

§ 13 Besondere Datenkategorien

(1) Emblon nimmt an den eingereichten Inhalten keine Vorprüfung, Bereinigung, Schwärzung oder sonstige Filterung vor, sondern verarbeitet sie im Rahmen der Diagnostik so, wie sie eingehen, und ausschließlich zu deren Zweck. Der Verantwortliche entscheidet allein, welche Dokumente und E-

Mail-Inhalte er übermittelt, und bleibt hierfür der datenschutzrechtlich Verantwortliche; die Rechtmäßigkeit der Einreichung richtet sich nach § 12. Die Diagnostik ist nicht auf besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) ausgerichtet; enthält eine Einreichung solche oder sonstige über den Prüfzweck hinausgehende personenbezogene Daten, so gelten Absatz 2 und 3.

(2) Stellt Emblon fest, dass eingereichte Unterlagen erkennbar Daten nach Absatz 1 enthalten, ist Emblon berechtigt, das betreffende Dokumentenpaket ganz oder teilweise von der Diagnostik auszunehmen und unverzüglich zu löschen; Emblon informiert den Verantwortlichen hierüber. Eine inhaltliche Sichtung aller Dokumente auf solche Daten schuldet Emblon nicht.

(3) Reicht der Verantwortliche entgegen Absatz 1 solche Daten ein, geschieht dies ohne Weisung und auf sein Risiko. § 12 Abs. 3 gilt entsprechend. Die Pflichten von Emblon aus §§ 4, 5 und 10 bleiben auch für unverlangt eingereichte Inhalte unberührt.

§ 14 Kein KI-Training; anonymisierte Leistungsdaten

(1) **Kein Training**. Emblon verwendet die Daten und Dokumente des Verantwortlichen nicht zum Training, zum Fine-Tuning oder zur sonstigen Fortentwicklung von KI-Modellen – weder eigener Modelle noch der Modelle Dritter. Emblon setzt ausschließlich Dienste ein, bei denen der Anbieter vertraglich zusichert, Kundendaten nicht zum Training seiner Modelle zu verwenden (Anlage 3). Ein- und Ausgaben der KI-gestützten Extraktion verbleiben in der Verfügungsgewalt von Emblon.

(2) **Qualitätsmessung nur anonymisiert**. Zur Messung und Verbesserung der Genauigkeit des eigenen Extraktions- und Prüfverfahrens darf Emblon ausschließlich **anonymisierte Leistungsdaten** erheben und zeitlich unbegrenzt aufbewahren. Anonymisiert sind Daten nur, wenn der Personenbezug irreversibel aufgehoben ist, d. h. wenn eine Identifizierung betroffener Personen auch unter Berücksichtigung aller Mittel, die nach vernünftigem Ermessen von Emblon oder einem Dritten wahrscheinlich genutzt werden (Erwägungsgrund 26 zur DSGVO), nicht mehr möglich ist. Eine bloße Pseudonymisierung (Art. 4 Nr. 5 DSGVO) – die Ersetzung von Identifikatoren bei fortbestehender Zuordnungsmöglichkeit mittels eines Schlüssels – genügt nicht und findet zu diesem Zweck nicht statt.

(3) Zulässige Leistungsdaten sind ausschließlich aggregierte oder strukturbezogene Kennzahlen ohne Klartextinhalte, insbesondere: Trefferquoten je Feldtyp (z. B. „Rechnungsnummer korrekt erkannt: ja/nein"), Fehlerklassen, Dokumenttyp- und Layoutstatistiken, Seitenzahlen, Verarbeitungszeiten und Konfidenzwerte. **Nicht** aufbewahrt werden: Dokumentbilder oder -kopien, Freitextauszüge, Namen, Kontaktdaten, IBAN oder sonstige Kontodaten, Rechnungs- oder Kundennummern sowie jede Kombination von Merkmalen, die eine Wiederherstellung des Personenbezugs ermöglichen würde. Die Anonymisierung erfolgt vor Ablauf der Löschfrist nach § 10; danach existiert keine Verbindung mehr zwischen Leistungsdaten und Quelldokumenten oder dem Verantwortlichen.

(4) Die Absätze 1 bis 3 sind zugleich Weisung im Sinne des § 3 und vertragliche Hauptpflicht.

§ 15 Haftung

(1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Innenverhältnis haften die Parteien einander entsprechend ihren Verantwortungsbeiträgen (Art. 82 Abs. 5 DSGVO); die Freistellungen nach § 12 Abs. 3 und § 13 Abs. 3 bleiben unberührt.

(2) Im Übrigen haftet Emblon dem Verantwortlichen unbeschränkt bei Vorsatz und grober Fahrlässigkeit sowie bei Verletzung von Leben, Körper oder Gesundheit. Bei einfach fahrlässiger Verletzung wesentlicher Vertragspflichten (Pflichten, deren Erfüllung die ordnungsgemäße Durchführung der Vereinbarung überhaupt erst ermöglicht und auf deren Einhaltung der Verantwortliche regelmäßig vertrauen darf) ist die Haftung auf den vertragstypischen, vorhersehbaren Schaden begrenzt; im Übrigen ist die Haftung für einfache Fahrlässigkeit ausgeschlossen. Zwingende gesetzliche Haftung bleibt unberührt.

§ 16 Schlussbestimmungen

(1) Diese Vereinbarung geht in Datenschutzfragen sonstigen Abreden über die Diagnostik vor. Änderungen und Ergänzungen bedürfen der Textform.

(2) Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist, soweit gesetzlich zulässig, Düsseldorf.

(3) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt; an die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand und Zweck: Einmalige diagnostische Prüfung von Eingangsrechnungen des Verantwortlichen und zugehörigen Nachweisen anhand eines regelbasierten Prüfrasters mit KI-gestützter Datenextraktion; Erstellung und Zustellung eines Diagnoseberichts an die verifizierte E-Mail-Adresse des Verantwortlichen.

Art der Verarbeitung: Entgegennahme der Dokumente (Upload oder E-Mail-Weiterleitung); Speicherung; KI-gestützte Extraktion der in den Dokumenten und E-Mails enthaltenen Angaben in einen standardisierten Datenbestand; KI-gestützte Einordnung des jeweiligen Dokumentenpakets in eine Rechnungs-Fallgruppe (Anwendungsfall); anschließende regelbasierte Prüfung durch eine Regel-Engine, die das im Einzelfall vorgesehene Vorgehen bestimmt; Erstellung und Übermittlung des Diagnoseberichts; Löschung. Die KI-gestützten Schritte dienen ausschließlich der Aufbereitung und Einordnung der Dokumentenpakete; eine Bewertung einzelner betroffener Personen findet nicht statt.

Automatisierte Entscheidungsfindung (Art. 22 DSGVO): Nein. Die automatisierten Schritte (Extraktion, Fallgruppen-Einordnung, regelbasierte Prüfung) beziehen sich auf die Rechnungs- und Nachweispakete des Verantwortlichen, nicht auf die Bewertung betroffener Personen. Sie entfalten keine rechtliche Wirkung und keine vergleichbar erhebliche Beeinträchtigung gegenüber betroffenen Personen; der Diagnosebericht dient allein der Auswertung für den Verantwortlichen.

Arten personenbezogener Daten:
- Identifikations- und Kontaktdaten von Ansprechpartnern und Inhabern der Lieferanten (Name, Funktion, dienstliche Adresse, E-Mail, Telefon);
- Zahlungs- und Abrechnungsdaten (IBAN/BIC, Rechnungs-, Kunden- und Steuernummern, Beträge);
- in Leistungs- und Stundennachweisen: Namen bzw. Kürzel eingesetzter Personen, Einsatzdaten, Zeiten, Tätigkeitsbeschreibungen, Qualifikations- und Zertifikatsangaben;
- Metadaten weitergeleiteter E-Mails (Absender, Empfänger, Zeitstempel, Betreff).

Kategorien betroffener Personen: Ansprechpartner, Inhaber und Beschäftigte der Lieferanten und Dienstleister des Verantwortlichen; Beschäftigte des Verantwortlichen, soweit sie in den Dokumenten oder als Absender erscheinen.

Besondere Datenkategorien: Nicht Gegenstand der Verarbeitung; Einreichung untersagt (§ 13).

Dauer: Von der Einreichung bis zur Löschung nach § 10 (spätestens 30 Tage nach Zustellung des Berichts zuzüglich Sicherungszyklen).

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

1. Verschlüsselung
- Transportverschlüsselung sämtlicher Übertragungswege mit TLS 1.2 oder höher (Upload, E-Mail-Eingang via MTA-STS/TLS, interne Dienstkommunikation, Berichtszustellung).
- Verschlüsselung aller gespeicherten Daten im Ruhezustand (AES-256; Azure Storage Service Encryption, transparente Datenverschlüsselung der PostgreSQL-Datenbank).

2**. Zugangs- und Zugriffskontrolle**
- Verarbeitung ausschließlich in dedizierten Azure-Abonnements von Emblon; rollenbasierte Zugriffskontrolle (RBAC) nach dem Prinzip der minimalen Berechtigung.
- Administrativer Zugang nur mit Multi-Faktor-Authentifizierung; personenbezogene Administratorkonten; keine geteilten Zugangsdaten.
- Geheimnisse (Schlüssel, Verbindungsdaten) in verwaltetem Schlüsselspeicher, nicht im Quellcode.

3. Eingabekontrolle und Mandantentrennung
- Zuordnung eingereichter Dokumente ausschließlich zum jeweiligen verifizierten Absender; logische Trennung der Datenbestände verschiedener Verantwortlicher.
- Annahme von E-Mail-Einreichungen nur von zuvor verifizierten Absenderadressen (Absender-Whitelisting mit SPF-/DKIM-/DMARC-Prüfung); nicht zuordenbare Eingänge werden verworfen und gelöscht.
- Protokollierung von Eingang, Verarbeitung, Berichtversand und Löschung.

4. Verfügbarkeit und Belastbarkeit
- Betrieb auf der Microsoft-Azure-Plattform ausschließlich in Rechenzentrumsregionen innerhalb der EU bzw. des EWR (derzeit Sweden Central) mit den dortigen Redundanz- und Wiederherstellungsmechanismen; kurzzyklische Sicherungen mit begrenzter Aufbewahrung entsprechend § 10.

5. Datenminimierung und Löschung
- Kein Export von Quelldaten aus der EU-Umgebung; keine lokalen Kopien auf Endgeräten.
- Automatisierte Löschroutine gemäß § 10 mit Protokollierung; Löschkonzept dokumentiert.
- KI-gestützte Extraktion ausschließlich über von Microsoft in der EU bereitgestellte Sprachmodelle innerhalb von Azure AI Foundry in EU-Bereitstellung („Standard"-Regionalbereitstellung bzw. „Data Zone Standard (EUR)"); keine Nutzung globaler Bereitstellungen; keine Verwendung der Inhalte zum Modelltraining durch den Anbieter.

6. Organisatorische Maßnahmen
- Verpflichtung aller befugten Personen zur Vertraulichkeit (§ 4); dokumentierte Verfahrensbeschreibung; Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO; Verfahren zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen (§ 9); regelmäßige Überprüfung der Wirksamkeit der Maßnahmen.

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Verarbeitungsort
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Cloud-Infrastruktur und Plattformdienste: Azure App Service, Azure Container Apps, Azure Database for PostgreSQL, Azure Blob Storage und Azure Queue Storage, Azure AI Foundry (KI-gestützte Extraktion mittels in der EU betriebener Sprachmodelle), Microsoft Graph / Exchange Online (E-Mail-Eingang und Berichtsversand)	Ausschließlich EU-/EWR-Rechenzentren (derzeit Region Sweden Central; KI-Bereitstellung: EU-regional bzw. Data Zone EU, keine globalen Bereitstellungen; Microsoft-365-Mandant mit Datenspeicherort EU)

Klarstellung: Die für die Extraktion eingesetzten Sprachmodelle werden ausschließlich innerhalb der Azure-Infrastruktur von Microsoft in der EU betrieben; die jeweiligen Modellanbieter erhalten keinen Zugriff auf Daten des Verantwortlichen und sind keine Unterauftragsverarbeiter. Microsoft sichert vertraglich zu, die verarbeiteten Inhalte nicht zum Training von KI-Modellen zu verwenden. Emblon kann die eingesetzten Modelle wechseln oder parallel betreiben, solange sie von Microsoft innerhalb der EU bereitgestellt werden und dieser Vereinbarung unterliegen; eine hierdurch etwaig hinzutretende weitere Stelle wird nach § 6 Abs. 2 behandelt.