Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

Dienstnutzer

- Verantwortlicher, im Folgenden **Auftraggeber** genannt -

und der

IT-SCom GmbH, Hertingerstr. 45, 59423 Unna, Deutschland

- Auftragsverarbeiter, im Folgenden **Auftragnehmer** genannt -

---

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Vertragsverhältnis über die Bereitstellung und den Betrieb der cloudbasierten Software-as-a-Service-Anwendung **„Freigado"** zur Übermittlung von Dokumenten an externe Empfänger zur Freigabe bzw. Prüfung ergeben.

Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit der zugrundeliegenden Leistungsbeschreibung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten (Daten) des Auftraggebers in Berührung kommen können.

---

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand des Auftrags und damit Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten ist die **Bereitstellung und der Betrieb der SaaS-Anwendung „Freigado"** durch den Auftragnehmer. Freigado ermöglicht es dem Auftraggeber, PDF-Dokumente hochzuladen und über einen signierten Einmal-Link an externe Empfänger zur Freigabe oder Prüfung zu übermitteln. Die Verarbeitung umfasst insbesondere:

- Speicherung und Bereitstellung der hochgeladenen Dokumente zur Ansicht durch den Empfänger;
- Verwaltung der Absender-Konten (Registrierung, Authentifizierung, E-Mail-Verifikation);
- Identitätsverifikation der Empfänger über einen per E-Mail versandten Einmalcode (OTP), ohne dass Empfänger ein dauerhaftes Nutzerkonto benötigen;
- Versand transaktionaler E-Mails (Einladungs-, Bestätigungscode- und Bestätigungs-E-Mails);
- Entgegennahme und Protokollierung der Empfänger-Entscheidung (Freigabe/Ablehnung) nebst optionalem Kommentar;
- revisionssichere Protokollierung der Verarbeitungsschritte (Audit-Log);
- **sofortige Löschung des Dokuments aus dem Speicher nach getroffener Entscheidung** sowie automatischer Ablauf nicht entschiedener Vorgänge.

Die Verarbeitung und Nutzung der Daten findet **ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum** statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, verbindliche interne Datenschutzvorschriften, Standarddatenschutzklauseln, genehmigte Verhaltensregeln, genehmigter Zertifizierungsmechanismus).

1.2 Dauer

Die Dauer dieser Vereinbarung (Laufzeit) richtet sich nach der Laufzeit der Leistungsbuchung bzw. des Abonnements im Rahmen des jeweiligen Produktvertrages (Freigado). Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

---

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Datenverarbeitung

Zweck der Datenerhebung, -verarbeitung und -nutzung ist der Betrieb der SaaS-Anwendung Freigado, d. h. die Speicherung, Bereitstellung, Verifikation, Benachrichtigung und Löschung von Dokumenten und zugehörigen Daten im Auftrag des Auftraggebers im Rahmen des Dokumenten-Freigabe-Prozesses. **Inhalt und Umfang der in den hochgeladenen Dokumenten enthaltenen personenbezogenen Daten werden allein vom Auftraggeber bestimmt;** der Auftragnehmer nimmt vom Inhalt der Dokumente keine inhaltliche Kenntnis und verarbeitet sie ausschließlich technisch zur Erbringung der Leistung.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind Daten aus folgenden Datenkategorien:

- **Konto-/Stammdaten der Absender** (Name, E-Mail-Adresse, gehashtes Passwort, Organisationszuordnung, Tarif/Abrechnungsstatus);
- **E-Mail-Adressen der Empfänger** (externe Prüfer);
- **Inhalt der hochgeladenen Dokumente** (PDF), die nach Bestimmung des Auftraggebers beliebige personenbezogene Daten enthalten können;
- **Vorgangs-/Metadaten** (Dateiname, Zeitstempel, Status, getroffene Entscheidung, optionaler Freitext-Kommentar);
- **Verifikationsdaten** (per E-Mail versandte Einmalcodes – ausschließlich gehasht gespeichert, mit kurzer Gültigkeit);
- **Protokoll-/Audit-Daten** (IP-Adresse, User-Agent, Zeitstempel der Erstellung, Verifikation, Entscheidung und Löschung).

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- **Beschäftigte/Nutzer des Auftraggebers** (Absender mit Konto);
- **externe Empfänger/Prüfer** (z. B. Geschäftspartner, Mandanten, Kunden, Behörden, sonstige Dritte);
- **in den hochgeladenen Dokumenten genannte oder erkennbare Personen** (Kategorie und Umfang werden allein durch den Auftraggeber bzw. den Dokumenteninhalt bestimmt).

---

3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, Anfragen von Betroffenen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

3.2 Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich per E-Mail oder Ticket-System oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

3.3 Der Auftraggeber ist berechtigt, sich wie unter Ziffer 8 festgelegt, vor Beginn der Datenverarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

3.4 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

3.5 Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

3.6 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

---

4 Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Sofern der Auftragnehmer zu einer anderen Verarbeitung gesetzlich verpflichtet ist, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine vom Auftraggeber erteilte Weisung gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Umsetzung der entsprechenden Weisung solange auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wurde.

4.3 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Eine Auswertung oder Nutzung der Dokumenteninhalte zu eigenen Zwecken (z. B. Training von KI-Modellen) findet nicht statt.

4.4 Kopien oder Duplikate der personenbezogenen Daten wird der Auftragnehmer ohne Wissen des Auftraggebers nicht erstellen. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

4.5 Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.

4.6 Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von den Daten anderer Auftraggeber **logisch strikt getrennt** (Mandantentrennung) verarbeitet werden. Die Zuordnung erfolgt über eine eindeutige Organisations-/Mandantenkennung; eine Vermengung mit Datenbeständen anderer Mandanten findet nicht statt.

4.7 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers wird der Auftragnehmer im notwendigen Umfang mitwirken und den Auftraggeber soweit möglich angemessen unterstützen.

4.8 Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

4.9 Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und in geeigneter Weise zur Verschwiegenheit verpflichtet – auch über die Beendigung des Beschäftigungsverhältnisses hinaus.

4.10 Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

4.11 Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

---

5 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

5.1 Dem Auftragnehmer ist bekannt, dass im Falle von Verletzungen des Schutzes personenbezogener Daten für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann (Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden).

5.2 Der Auftragnehmer wird dem Auftraggeber daher unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie einen Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung mitteilen.

5.3 Der Auftragnehmer trifft angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

5.4 Der Auftragnehmer wird den Auftraggeber erforderlichenfalls bei entsprechenden Meldepflichten angemessen unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung vornehmen.

---

6 Unterauftragsverhältnisse mit Subunternehmern

6.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit (auch elektronischer) Zustimmung des Auftraggebers gestattet. Mit Abschluss dieser Vereinbarung stimmt der Auftraggeber den in **Anlage 2** genannten Subunternehmern zu.

6.2 Eine Beauftragung von Subunternehmern, die die vereinbarten Leistungen außerhalb der EU/des EWR erbringen, darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. **Die derzeit eingesetzten Subunternehmer (Anlage 2) verarbeiten ausschließlich innerhalb der EU/des EWR.**

6.3 Der Auftragnehmer hat vertraglich sicherzustellen, dass die zwischen Auftraggeber und Auftragnehmer vereinbarten Regelungen auch gegenüber Subunternehmern gelten, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen im Sinne von Art. 28 Abs. 4, Art. 32 DSGVO.

6.4 Der Vertrag mit dem Subunternehmer ist schriftlich (auch elektronisch) abzufassen.

6.5 Die Weitergabe personenbezogener Daten an den Unterauftragnehmer ist erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.6 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den ihm vertraglich auferlegten Datenschutzpflichten nachkommt.

6.7 Zurzeit sind für den Auftragnehmer die in **Anlage 2** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

6.8 Vor der Hinzuziehung weiterer oder der Ersetzung bisheriger Subunternehmer wird der Auftragnehmer den Auftraggeber rechtzeitig (auch elektronisch) informieren. Der Auftraggeber kann der Änderung innerhalb von zehn Werktagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung als erteilt. Ist bei berechtigtem Widerspruch keine einvernehmliche Lösung möglich, erhält der Auftraggeber ein Sonderkündigungsrecht.

6.9 Eine weitere Auslagerung durch einen Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers; sämtliche vertraglichen Regelungen der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

---

7 Technisch-organisatorische Maßnahmen

7.1 Der Auftragnehmer gewährleistet für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau.

7.2 Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Sinne von Art. 32 DSGVO.

7.3 Die in **Anlage 1** dokumentierten Maßnahmen stellen die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko dar.

7.4 Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen durchzuführen.

7.5 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

7.6 Die Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

7.7 Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form abstimmen und für die Dauer des Vertrages aufbewahren.

---

8 Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber ist – grundsätzlich nach Terminvereinbarung – berechtigt, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen beim Auftragnehmer im angemessenen und erforderlichen Umfang zu kontrollieren, insbesondere durch Einholung von Auskünften und Einsichtnahme sowie durch Überprüfungen und Inspektionen. Der Nachweis kann auch durch aktuelle Testate, Zertifikate oder Berichte unabhängiger Instanzen geführt werden.

8.2 Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen, um die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig zu stören.

8.3 Der Auftragnehmer sichert zu, dass er bei diesen Kontrollen unterstützend mitwirkt und die Umsetzung der technischen und organisatorischen Maßnahmen nachweist.

8.4 Für die Ermöglichung von Kontrollen kann der Auftragnehmer bei unverhältnismäßigem Aufwand einen angemessenen Vergütungsanspruch geltend machen.

---

9 Berichtigung, Einschränkung und Löschung von Daten

9.1 Der Auftragnehmer darf die im Auftrag verarbeiteten Daten nicht eigenmächtig, sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Hiervon unberührt bleibt die im Dienst systemseitig vorgesehene **automatische Löschung** der Dokumente nach getroffener Entscheidung sowie der Ablauf nicht entschiedener Vorgänge, die Bestandteil der vereinbarten Leistung sind.

9.2 Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter. Auskünfte an Dritte oder Betroffene erteilt der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung des Auftraggebers.

---

10 Verpflichtungen nach Beendigung des Auftrags

10.1 Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung, spätestens mit Beendigung des Hauptvertrages, hat der Auftragnehmer sämtliche in seinen Besitz sowie an

Unterauftragnehmer gelangten Daten und Verarbeitungsergebnisse dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu löschen bzw. zu vernichten.

10.2 Die Löschung bzw. Vernichtung ist dem Auftraggeber auf Anforderung mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

---

11 Haftung

Eine zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, es sei denn, es ist ausdrücklich etwas anderes vereinbart.

---

12 Schlussbestimmungen

12.1 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform (auch elektronisch) und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

12.2 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Hauptvertrages vor.

12.3 Es gilt deutsches Recht unter Ausschluss des materiellen internationalen Privat- sowie Kollisionsrechts.

12.4 Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der Vereinbarung im Übrigen unberührt.

Die folgenden Anlagen gelten als vertragswesentliche Bestandteile:

- **Anlage 1** – Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
- **Anlage 2** – Genehmigte Subunternehmer

.....

- Auftragnehmer (IT-SCom GmbH)

.....

- Auftraggeber

Anlage 1 — Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Verantwortliche Stelle (Auftragnehmer): IT-SCom GmbH, Hertingerstr. 45, 59423 Unna, Deutschland

> Die physische Sicherheit der Rechenzentren (Zutritt, Brandschutz, USV, Redundanz) wird durch die in Anlage 2 genannten EU-Hosting-Dienstleister (Clever Cloud, IONOS) im Rahmen ihrer Zertifizierungen gewährleistet. Der Auftragnehmer setzt die nachstehenden organisatorischen sowie anwendungs- und betriebsseitigen Maßnahmen um.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zugangskontrolle (Zugang zur Anwendung):

- Authentifizierung der Absender mit E-Mail und Passwort; **verpflichtende E-Mail-Verifikation per Einmalcode** bei der Registrierung
- Passwörter werden ausschließlich als kryptografischer Hash gespeichert
- Empfänger-Zugang ausschließlich über einen **kryptografisch signierten Einmal-Link** und zusätzliche **Identitätsverifikation per E-Mail-Einmalcode (OTP)**; kein dauerhaftes Empfänger-Konto erforderlich (Datensparsamkeit)
- Rollenbasierte Rechte (Administrator/Nutzer); Reduktion administrativer Zugänge auf das Notwendige
- Selbst gehostete Authentifizierung (keine Auslagerung der Authentifizierung an Drittanbieter außerhalb der EU)

Zugriffskontrolle:

- Berechtigungskonzept; Zugriff auf Daten nur im erforderlichen Umfang
- **Verschlüsselung in der Übertragung** (TLS/HTTPS) sowie **Verschlüsselung im ruhenden Zustand** (Objektspeicher und Datenbank der EU-Hosting-Dienstleister)
- Protokollierung von Zugriffen und sicherheitsrelevanten Vorgängen (Audit-Log)
- Sichere Passwörter und Passwortrichtlinien

Trennungsgebot / Mandantentrennung:

- Logische Mandantentrennung über eindeutige Organisations-/Mandantenkennung (softwareseitig)
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Test-/Entwicklungssystem

Pseudonymisierung / Datenminimierung:

- In Entwicklungs-/Test-/Analyseumgebungen werden keine Produktivdaten verwendet bzw. nur pseudonymisiert/anonymisiert, soweit technisch möglich
- Empfänger werden ohne dauerhaftes Konto und nur über E-Mail-Adresse + Einmalcode verifiziert

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle:

- Verschlüsselte Übertragung (TLS/HTTPS)
- Manipulationssichere, **signierte Einmal-Links** (HMAC); Zugriff auf das Dokument erst nach erfolgreicher OTP-Verifikation
- Sofortige Löschung des Dokuments aus dem Speicher nach getroffener Entscheidung

Eingabekontrolle:

- Nachvollziehbarkeit von Erstellung, Verifikation, Entscheidung und Löschung durch revisionssicheres **Audit-Log** (wer, wann, von welcher IP-Adresse, User-Agent)
- Vergabe von Eingabe-/Änderungs-/Löschrechten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Automatische Datensicherung der Datenbank (Managed-Backups des EU-Hosting-Dienstleisters)
- Redundante Speicherung der Objektdaten beim EU-Objektspeicher-Dienstleister
- Physische Verfügbarkeitsmaßnahmen der Rechenzentren (USV, Brand-/Rauchmeldung, Klimatisierung) durch die EU-Hosting-Dienstleister gemäß deren Zertifizierungen
- Notfall-/Wiederherstellungskonzept; Test der Wiederherstellung

4. Besondere Maßnahmen zur Speicherbegrenzung / Löschung (Art. 5 Abs. 1 lit. e, Art. 25 DSGVO)

- **Sofortige Löschung** des hochgeladenen Dokuments aus dem Objektspeicher unmittelbar nach der Entscheidung des Empfängers
- **Automatischer Ablauf** nicht entschiedener Vorgänge (Standard: 30 Tage) mit anschließender Löschung des Dokuments durch einen geplanten Bereinigungsprozess
- Einmalcodes werden nur gehasht und mit kurzer Gültigkeit gespeichert
- Definierte Aufbewahrungsfrist für Metadaten/Audit-Daten (revisionssicher), danach Löschung

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

- IT-Sicherheitskonzept; regelmäßige Überprüfung und Evaluierung der Maßnahmen
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Revision der Datenverarbeitung; anlassbezogene bzw. regelmäßige Sicherheitsprüfungen (z. B. Penetrationstests)

Anlage 2 — Genehmigte Subunternehmer

> Sämtliche nachstehenden Subunternehmer verarbeiten **ausschließlich innerhalb der EU/des EWR**. Es findet **keine Drittlandübermittlung** und es werden **keine US-Subprozessoren** eingesetzt. (Firmierung/Anschrift vor Verwendung verifizieren.)

Name und Anschrift des Subunternehmers	Auftragsinhalt	Verarbeitungsort
Clever Cloud SAS, 4 rue Voltaire, 44000 Nantes, Frankreich	Hosting der Web-Anwendung und der PostgreSQL-Datenbank (Application Platform)	Frankreich (EU)
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland	S3-kompatibler Objektspeicher für die hochgeladenen Dokumente	Deutschland (EU)
Brevo GmbH, Köpenicker Straße 126, 10179 Berlin, Deutschland	Versand transaktionaler E-Mails (Einladungs-, Bestätigungscode- und Bestätigungs-E-Mails)	EU

Stand: 11.06.2026