Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

(Auftragsverarbeitungsvertrag – AVV) nach Art. 28 DSGVO

Fassung: September 2026, Version 1.2

Zwischen

[Organisation / Behörde]
[Straße und Hausnummer]
[PLZ] [Ort]
[Land]

vertreten durch die Person, die diesen Vertrag über das Kundenkonto (Organisation) in der Anwendung LVision digital bestätigt. Name und E-Mail-Adresse dieser Person sowie der Zeitpunkt der Bestätigung werden vom Auftragnehmer zusammen mit dieser Vertragsfassung protokolliert.

– nachfolgend **„Verantwortlicher"** –

und

Baulytics GmbH Im Feldchen 14 35043 Marburg vertreten durch die Geschäftsführer Guido Irmischer und Sebastian Gruber Amtsgericht Marburg, HRB 8996

– nachfolgend **„Auftragnehmer"** –

– gemeinsam die **„Parteien"** –

Präambel

Der Auftragnehmer stellt dem Verantwortlichen die Software-as-a-Service-Anwendung **LVision** zur automatisierten Prüfung von Leistungsverzeichnissen (LV) auf Grundlage der Allgemeinen Geschäftsbedingungen (AGB) für LVision in ihrer jeweils geltenden Fassung bereit (nachfolgend **„Hauptvertrag"**). Im Rahmen dieser Leistungserbringung verarbeitet der Auftragnehmer personenbezogene Daten, die in den vom Verantwortlichen hochgeladenen Dokumenten enthalten sind, im Auftrag und nach Weisung des Verantwortlichen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien nach Art. 28 DSGVO. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags in datenschutzrechtlichen Fragen vor.

§ 1 Gegenstand, Dauer und Art der Verarbeitung

(1) Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich abschließend aus **Anlage 1** zu diesem Vertrag.

(2) Die Verarbeitung erfolgt ausschließlich auf dem Gebiet der Europäischen Union oder des Europäischen Wirtschaftsraums. Eine Verarbeitung in einem Drittland findet nur nach Maßgabe von § 8 und nur unter den dort genannten Voraussetzungen statt.

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags, sofern sich aus den Regelungen dieses Vertrags – insbesondere zu Löschung und Rückgabe (§ 11) – keine darüber hinausgehenden Pflichten ergeben.

(4) Nicht Gegenstand dieses Vertrags sind personenbezogene Daten, die der Auftragnehmer als eigener Verantwortlicher verarbeitet. Dies betrifft insbesondere die Konto-, Vertrags-, Abrechnungs- und Zahlungsdaten des Verantwortlichen und seiner Nutzer sowie die Support-Kommunikation. Hierfür gilt die Datenschutzerklärung von LVision.

§ 2 Weisungsrecht des Verantwortlichen

(1) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Verantwortlichen, einschließlich in Bezug auf die Übermittlung an ein Drittland, es

sei denn, er ist hierzu nach dem Recht der Union oder eines Mitgliedstaats verpflichtet (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Nutzung der Funktionen von LVision (insbesondere Hochladen, Analysieren, Herunterladen und Löschen von Dokumenten und Analysen) gilt als Weisung des Verantwortlichen. Darüber hinausgehende Weisungen werden in Textform an die E-Mail-Adresse info@baulytics.de erteilt. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Weisungsberechtigte und weisungsempfangende Personen sind in **Anlage 1** benannt.

(3) Der Auftragnehmer informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs. 3 Satz 2 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.

---

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich gemäß den Weisungen des Verantwortlichen und zu den vertraglich vereinbarten Zwecken. Eine Verarbeitung zu eigenen Zwecken findet nicht statt. Insbesondere werden hochgeladene Dokumente und Analyseergebnisse nicht zum Training von KI-Modellen verwendet.

(2) Der Auftragnehmer gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO). Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(3) Der Auftragnehmer ergreift alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in **Anlage 2** beschrieben (§ 4).

(4) Der Auftragnehmer unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung der Betroffenenrechte (§ 6) sowie der Pflichten aus Art. 32 bis 36 DSGVO (§ 7).

(5) Der Auftragnehmer ist derzeit nicht zur Benennung eines Datenschutzbeauftragten verpflichtet und hat keinen benannt. Ansprechstelle für Datenschutzfragen ist die Geschäftsführung, erreichbar unter info@baulytics.de. Sollte künftig ein Datenschutzbeauftragter benannt werden, teilt der Auftragnehmer dessen Kontaktdaten in der Datenschutzerklärung von LVision mit.

(6) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung der personenbezogenen Daten nur auf Weisung des Verantwortlichen ein, es sei denn, eine gesetzliche Verpflichtung verlangt anderes.

(7) Der Auftragnehmer führt, soweit nach Art. 30 Abs. 2 DSGVO erforderlich, ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten.

---

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

(1) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist es gestattet, alternative, angemessene Maßnahmen umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Verantwortlichen auf Anfrage nachzuweisen.

---

§ 5 Inanspruchnahme weiterer Auftragsverarbeiter (Subunternehmer)

(1) Der Verantwortliche erteilt dem Auftragnehmer die **allgemeine schriftliche Genehmigung** zur Inanspruchnahme weiterer Auftragsverarbeiter (Art. 28 Abs. 2 Satz 1 Alt. 2 DSGVO). Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmer sind in **Anlage 3** abschließend aufgeführt; der Verantwortliche genehmigt deren Einsatz mit Abschluss dieses Vertrags.

(2) Der Auftragnehmer informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter mit einer Frist von mindestens 14 Tagen vor der Beauftragung. Die Information erfolgt per E-Mail an die Nutzer mit der Rolle „Inhaber" oder „Admin" im Kundenkonto des Verantwortlichen sowie durch Aktualisierung der Anlage 3 in der Anwendung. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen (Art. 28 Abs. 2 Satz 2 DSGVO).

(3) Widerspricht der Verantwortliche fristgerecht und aus wichtigem Grund, und kann der Auftragnehmer die Leistung ohne den betreffenden Subunternehmer nicht zu wirtschaftlich zumutbaren Bedingungen erbringen, sind beide Parteien zur außerordentlichen Kündigung des betroffenen Leistungsbestandteils berechtigt.

(4) Der Auftragnehmer verpflichtet jeden weiteren Auftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die in diesem Vertrag festgelegt sind, insbesondere auf hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragnehmer gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses weiteren Auftragsverarbeiters.

(5) Nicht als Subunternehmer im Sinne dieser Vorschrift gelten Nebenleistungen, die der Auftragnehmer als reine Hilfsleistung in Anspruch nimmt (etwa Telekommunikations-, Post-, Transport-, Wartungs- und Reinigungsdienste). Der Auftragnehmer ist jedoch verpflichtet, auch hierbei den Schutz der personenbezogenen Daten zu gewährleisten.

---

§ 6 Unterstützung bei Betroffenenrechten

(1) Macht eine betroffene Person Rechte nach Art. 12 bis 22 DSGVO (insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) unmittelbar gegenüber dem Auftragnehmer geltend, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.

(2) Der Auftragnehmer unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nachzukommen (Art. 28 Abs. 3 lit. e DSGVO), insbesondere durch die Funktionen der Anwendung zum Abruf und zur Löschung von Dokumenten und Analysen sowie durch Auskünfte und die Durchführung von Berichtigungen und Löschungen auf Weisung.

---

§ 7 Unterstützung bei Sicherheit, Meldepflichten und Folgenabschätzung

(1) Der Auftragnehmer unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten (Art. 28 Abs. 3 lit. f DSGVO).

(2) **Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 Abs. 2 DSGVO):** Der Auftragnehmer meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten **unverzüglich, in der Regel innerhalb von 48 Stunden** nach Bekanntwerden per E-Mail an die Nutzer mit der Rolle „Inhaber" oder „Admin" im Kundenkonto. Die Meldung enthält mindestens die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben, soweit dem Auftragnehmer bekannt: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, voraussichtliche Folgen sowie ergriffene oder vorgeschlagene Gegenmaßnahmen. Die Meldung an die Aufsichtsbehörde nach Art. 33 Abs. 1 DSGVO und die Benachrichtigung der Betroffenen nach Art. 34 DSGVO obliegen dem Verantwortlichen.

(3) Der Auftragnehmer unterstützt den Verantwortlichen bei einer etwaigen Datenschutz-Folgenabschätzung nach Art. 35 DSGVO sowie bei einer vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO, soweit dies aufgrund der Art der Verarbeitung und der dem Auftragnehmer vorliegenden Informationen erforderlich ist.

---

§ 8 Verarbeitung in Drittländern

(1) Eine Übermittlung oder Verarbeitung personenbezogener Daten in einem Drittland (außerhalb der EU/des EWR) oder durch eine internationale Organisation findet nur statt, soweit dies in **Anlage 3** ausdrücklich ausgewiesen ist und die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

(2) Die Verarbeitung erfolgt ausschließlich in der EU/im EWR (siehe Anlage 3). Soweit ein eingesetzter Subunternehmer einem Konzern mit Sitz in einem Drittland angehört und dadurch einem potenziellen Zugriff nach dortigem Recht (insbesondere US CLOUD Act, FISA 702) unterliegen kann, sichert der Auftragnehmer dieses Risiko durch geeignete technische, organisatorische und vertragliche Maßnahmen sowie durch die Datenschutzgarantien des jeweiligen Anbieters ab. Die Bewertung ist in **Anlage 4** dokumentiert.

(3) Soweit ausnahmsweise eine tatsächliche Übermittlung in ein Drittland stattfindet (etwa durch Fernzugriff des Anbieters im Support-Fall), stützt sich diese vorrangig auf einen Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO – für die USA den Durchführungsbeschluss (EU) 2023/1795 (EU-US Data Privacy Framework), sofern und solange der betreffende Anbieter entsprechend zertifiziert ist – und ergänzend auf die Standardvertragsklauseln der Kommission gemäß Durchführungsbeschluss (EU) 2021/914 (Art. 46 DSGVO), die mit dem Anbieter abgeschlossen sind und automatisch greifen, falls die Zertifizierung entfällt oder der Angemessenheitsbeschluss aufgehoben wird.

---

§ 9 Kontroll- und Nachweisrechte des Verantwortlichen

(1) Der Auftragnehmer stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Auftragnehmer ermöglicht Überprüfungen – einschließlich Inspektionen –, die der Verantwortliche oder ein von diesem beauftragter Prüfer durchführt, und trägt zu diesen bei. Der Nachweis kann auch durch die Vorlage geeigneter, aktueller Zertifizierungen, genehmigter Verhaltensregeln oder Berichte einer unabhängigen Instanz (etwa ISO/IEC 27001, SOC 2 Typ II, Testat eines Wirtschaftsprüfers) – auch der eingesetzten Subunternehmer – erbracht werden.

(3) Vor-Ort-Kontrollen sind mit angemessener Vorankündigung von mindestens zwei Wochen und zu den üblichen Geschäftszeiten durchzuführen, höchstens einmal jährlich, es sei denn, es bestehen konkrete Anhaltspunkte für einen Datenschutzverstoß oder eine Aufsichtsbehörde verlangt eine Prüfung. Der Verantwortliche trägt die ihm hierdurch entstehenden Kosten; ein über die gesetzliche Mitwirkung hinausgehender, gesondert beauftragter Prüfaufwand des Auftragnehmers kann nach vereinbartem Aufwand vergütet werden.

---

§ 10 Mitteilungspflichten

(1) Der Auftragnehmer informiert den Verantwortlichen unverzüglich über Kontrollmaßnahmen und Anordnungen einer Aufsichtsbehörde, soweit sie sich auf die Auftragsverarbeitung beziehen, sowie über behördliche Auskunftsersuchen zu den im Auftrag verarbeiteten Daten, soweit dies rechtlich zulässig ist.

(2) Der Auftragnehmer sichert zu, dass er den Verantwortlichen bei der Wahrung der Rechte betroffener Personen sowie bei aufsichtsbehördlichen Verfahren angemessen unterstützt.

---

§ 11 Löschung und Rückgabe nach Beendigung

(1) Nach Abschluss der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Der Verantwortliche kann hochgeladene Dokumente und Analyseergebnisse bis zum Vertragsende über die Anwendung abrufen. Er teilt seine Wahl (Löschung oder Rückgabe) spätestens innerhalb von 30 Tagen nach Vertragsende mit. Ohne ausdrückliche Wahl gilt nach Ablauf von 30 Tagen die Löschung als gewählt. Für eine Rückgabe stellt der Auftragnehmer die Daten in einem gängigen, strukturierten Datenformat bereit.

(3) Vom Verantwortlichen gelöschte Analysen und zugehörige Dateien – ebenso alle Analysen eines gelöschten Kundenkontos – werden nach einer Karenzzeit von 30 Tagen endgültig aus den Produktivsystemen entfernt. Die täglich erstellten, verschlüsselten und räumlich getrennt in Deutschland aufbewahrten Datensicherungen unterliegen einer rollierenden Aufbewahrungsfrist von höchstens 30 Tagen. Daten können daher bis zu 30 weitere Tage ausschließlich in Sicherungskopien enthalten sein; spätestens 60 Tage nach Einleitung der Löschung sind auch die letzten Sicherungskopien entfernt. Sicherungskopien werden ausschließlich zur Wiederherstellung nach einem technischen oder physischen Schadensereignis verwendet. Nach einer Wiederherstellung werden zwischenzeitlich fällige Löschungen erneut durchgeführt. Die Löschung erfolgt nach dem Stand der Technik und wird dem Verantwortlichen auf Anfrage in Textform bestätigt.

---

§ 12 Haftung

Für die Haftung der Parteien gelten die Regelungen des Hauptvertrags sowie ergänzend Art. 82 DSGVO. Im Außenverhältnis zu betroffenen Personen bleibt die gesetzliche Haftungsverteilung des Art. 82 DSGVO unberührt.

---

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags einschließlich seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Textformerfordernisses. Aktualisierungen der Anlagen 3 und 4 nach § 5 Abs. 2 und Anlage 4 Abschnitt E bleiben hiervon unberührt.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen und datenschutzrechtlichen Zweck am nächsten kommt.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist – soweit zulässig – Marburg.

---

§ 14 Vertragsschluss in elektronischer Form

(1) Dieser Vertrag wird geschlossen, indem eine hierzu berechtigte Person des Verantwortlichen (Nutzer mit der Rolle „Inhaber" oder „Admin" im Kundenkonto) ihn in der Anwendung LVision digital bestätigt. Der Auftragnehmer bietet den Abschluss mit Bereitstellung des Vertrags in der Anwendung an. Der Auftragnehmer protokolliert Kundenkonto, bestätigende Person und Zeitpunkt der Bestätigung und stellt den Vertrag beiden Parteien dauerhaft als PDF-Dokument zum Abruf bereit.

(2) Die digitale Bestätigung genügt dem elektronischen Format nach Art. 28 Abs. 9 DSGVO und der Textform nach § 126b BGB. Einer eigenhändigen Unterschrift bedarf es nicht.

(3) Die bestätigende Person sichert zu, zur Vertretung des Verantwortlichen beim Abschluss dieses Vertrags befugt zu sein.

Anlage 1 – Gegenstand und Einzelheiten der Verarbeitung

Gegenstand und Zweck der Verarbeitung

Bereitstellung der Software-as-a-Service-Anwendung LVision gemäß Hauptvertrag: Der Verantwortliche lädt Leistungsverzeichnisse (GAEB-Dateien, PDF-Dokumente und vergleichbare Dateien) hoch. LVision extrahiert deren Inhalte (einschließlich Texterkennung bei gescannten Dokumenten), prüft sie automatisiert und KI-gestützt auf fachliche, formale und vergaberelevante Befunde, erstellt Berichte und stellt Ergebnisse und Dateien zum Abruf bereit.

Art der Verarbeitung

Erheben (Upload), Speichern, Auslesen und Extrahieren, automatisierte Analyse einschließlich KI-Inferenz, Erstellen von Berichten, Bereitstellen zum Abruf, Löschen.

Art der personenbezogenen Daten

- Personenbezogene Daten, die in den hochgeladenen Dokumenten enthalten sind, insbesondere Namen, Funktionen, Anschriften, Telefonnummern, E-Mail-Adressen und Unterschriften von Projektbeteiligten (etwa Auftraggeber, Bauherren, Planer, Bieter, Nachunternehmer, Bauleitung, Behördenvertreter)
- Aus diesen Dokumenten extrahierte Inhalte, Zwischenergebnisse, Befunde und Berichte, soweit sie diese Daten enthalten
- Nutzungsmetadaten in Verbindung mit einer Analyse: Name und E-Mail-Adresse des hochladenden Nutzers, Zeitpunkte, Dateiname, Dateityp und Dateigröße, Analyseparameter und Verarbeitungsstatus

Kategorien betroffener Personen

- Beschäftigte und Ansprechpartner des Verantwortlichen
- Beschäftigte und Ansprechpartner Dritter, die in den hochgeladenen Dokumenten genannt sind (Auftraggeber, Bauherren, Planer, Bieter, Nachunternehmer, Behörden)
- Nutzer des Verantwortlichen in LVision

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

Keine. Die Verarbeitung besonderer Kategorien ist nicht vorgesehen; der Verantwortliche lädt keine Dokumente hoch, die solche Daten enthalten.

Weisungsberechtigte Personen des Verantwortlichen

Nutzer mit der Rolle „Inhaber" oder „Admin" im Kundenkonto des Verantwortlichen. Der Verantwortliche pflegt diesen Personenkreis selbst über die Organisationsverwaltung der Anwendung.

Weisungsempfänger beim Auftragnehmer

Geschäftsführung der Baulytics GmbH, E-Mail: info@baulytics.de

Datenschutzbeauftragter des Auftragnehmers

Nicht benannt, da nicht erforderlich. Ansprechstelle für Datenschutzfragen: info@baulytics.de

---

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

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

- *Zutrittskontrolle:* Die Produktivsysteme werden in Rechenzentren der netcup GmbH in Deutschland betrieben. Der Zutritt ist auf autorisiertes Personal des Rechenzentrumsbetreibers beschränkt und wird kontrolliert und protokolliert. Beschäftigte

des Auftragnehmers haben keinen physischen Zutritt zu den Servern.

- *Zugangskontrolle:* Individuelle Benutzerkonten, sichere Passwörter, begrenzte Anmeldeversuche und verpflichtende Mehr-Faktor-Authentifizierung für administrative und sonstige privilegierte Zugänge; Wiederherstellungscodes und Notfallzugänge werden gesondert geschützt aufbewahrt. Nutzerkonten erfordern eine verifizierte E-Mail-Adresse; Passwörter werden ausschließlich als Hash gespeichert; allen Nutzern steht eine Zwei-Faktor-Authentifizierung zur Verfügung. Zugangsdaten zu Diensten und Subunternehmern werden außerhalb des Quellcodes verwaltet.
- *Zugriffskontrolle:* Rollen- und Berechtigungskonzept innerhalb des Kundenkontos (Inhaber, Admin, Mitglied) mit serverseitiger Prüfung jeder Aktion. Administrative Funktionen des Auftragnehmers sind auf gesondert berechtigte Personen beschränkt. Beschäftigte des Auftragnehmers greifen auf Kundendaten nur zu, soweit dies für Betrieb, Support oder Fehlerbehebung erforderlich ist (Need-to-know-Prinzip).
- *Trennungskontrolle:* Logische Mandantentrennung: Alle Dokumente, Analysen und Ergebnisse sind einem Kundenkonto zugeordnet und nur dessen Mitgliedern zugänglich. Entwicklungs-, Test- und Produktivumgebungen sind getrennt; in Entwicklung und Test werden keine Produktivdaten verwendet.
- *Verschlüsselung:* Sämtliche Verbindungen zwischen Nutzern und LVision sowie zwischen LVision und den Subunternehmern (AWS-Schnittstellen) sind TLS-verschlüsselt. Sicherungskopien werden verschlüsselt gespeichert.

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

- *Weitergabekontrolle:* Datenübertragung ausschließlich über TLS-verschlüsselte Verbindungen. Der Abruf von Dokumenten, Berichten und Ergebnissen ist nur angemeldeten Mitgliedern des jeweiligen Kundenkontos möglich. Eine Weitergabe an Dritte außerhalb der in Anlage 3 genannten Subunternehmer findet nicht statt.
- *Eingabekontrolle:* Hochladen, Analysieren und Löschen von Dokumenten werden mit Nutzer- und Zeitbezug protokolliert. Lösch- und Aufbewahrungsläufe werden protokolliert. Die digitale Bestätigung dieses Vertrags wird mit Kundenkonto, Person und Zeitpunkt festgehalten.

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

- Tägliche automatisierte Sicherung der Datenbank sowie der persistent gespeicherten Kundendaten und Analyseergebnisse. Die Sicherungskopien werden verschlüsselt, räumlich getrennt vom Produktivsystem in Deutschland aufbewahrt und nach höchstens 30 Tagen automatisiert gelöscht beziehungsweise überschrieben.
- Das Wiederherstellungsverfahren wurde erfolgreich getestet. Die Wiederherstellbarkeit wird regelmäßig durch dokumentierte Wiederherstellungstests in einer vom Produktivsystem getrennten Umgebung überprüft; dabei verwendete Testkopien werden nach Abschluss des Tests gelöscht.
- Die Anwendung wird containerisiert mit Zustandsüberwachung (Healthchecks) und unterbrechungsfreien Aktualisierungen betrieben. Verarbeitungsaufträge werden über Warteschlangen mit automatischer Wiederholung bei Fehlern ausgeführt. Der Rechenzentrumsbetreiber stellt Netzwerkschutz, redundante Stromversorgung und Anbindung bereit.

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

- Datenschutzmanagement: dokumentiertes Löschkonzept, Datenschutzerklärung und dieser Vertrag werden bei Änderungen der Anwendung, der Subunternehmer oder der Rechtslage, mindestens jedoch jährlich, überprüft.
- Incident-Response: Meldeweg und Fristen nach § 7 Abs. 2 dieses Vertrags; Sicherheitsvorfälle werden dokumentiert und ausgewertet.
- Auftragskontrolle gegenüber Subunternehmern: Mit jedem Subunternehmer bestehen Vereinbarungen nach Art. 28 DSGVO; deren Zertifizierungen und Standorte werden mindestens jährlich überprüft.
- Datenschutz durch Technikgestaltung: Analysen und zugehörige Dateien werden auf Weisung des Verantwortlichen gelöscht und nach der Karenzzeit endgültig entfernt (§ 11 Abs. 3). An den KI-Dienst werden nur die für die Prüfung erforderlichen Dokumentinhalte übermittelt.

Zertifizierungen und Nachweise

Der Auftragnehmer verfügt derzeit über keine eigene Zertifizierung. Nachweise der Subunternehmer: netcup GmbH betreibt Rechenzentren in Deutschland und weist deren Sicherheitsmaßnahmen auf Anfrage nach; Amazon Web Services ist unter anderem nach ISO/IEC 27001, 27017 und 27018 zertifiziert und verfügt über SOC 1, 2 und 3 Berichte sowie ein BSI C5-Testat (abrufbar über AWS Artifact).

Anlage 3 – Liste der genehmigten Subunternehmer

Nr.	Subunternehmer	Vertragsentität	Leistung	Ort der Verarbeitung	Drittlandsbezug	Vertragliche Absicherung
1	netcup GmbH	netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe, Deutschland	Server- und Infrastruktur-Hosting (Anwendung, Datenbank, Dateispeicher, Sicherungskopien)	Deutschland	Nein	Auftragsverarbeitungsvertrag nach Art. 28 DSGVO
2	Amazon Web Services	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	KI-Inferenz (Amazon Bedrock) und E-Mail-Versand (Amazon SES)	AWS-Regionen innerhalb der EU; Bedrock über EU-Inferenzprofile (unter anderem Frankfurt, Irland, Paris), SES in Frankfurt (eu-central-1)	Verarbeitung in der EU; potenzielles Zugriffsrisiko über die US-Konzernmutter Amazon.com, Inc.	AWS GDPR Data Processing Addendum einschließlich Standardvertragsklauseln (EU) 2021/914; EU-US Data Privacy Framework (Amazon Web Services, Inc. ist zertifiziert); Bewertung in Anlage 4

Erläuterungen

1. **Eigenbetrieb:** Dokumentenkonvertierung, PDF-Erstellung, Datenbank, Zwischenspeicher und Warteschlangen betreibt der Auftragnehmer selbst auf der bei netcup gehosteten Infrastruktur. Hierfür werden keine weiteren Subunternehmer eingesetzt.
2. **Amazon Bedrock:** Die KI-Inferenz erfolgt ausschließlich in AWS-Regionen innerhalb der EU. Nach den Nutzungsbedingungen von AWS werden Eingaben und Ausgaben weder gespeichert noch an die Anbieter der Basismodelle weitergegeben noch zum Training von Modellen verwendet.
3. **Aktualität:** Die jeweils aktuelle Fassung dieser Liste ist in der Anwendung unter „Auftragsverarbeitungsvertrag" abrufbar. Änderungen werden nach § 5 Abs. 2 mitgeteilt.

Anlage 4 – Drittlandsbezug und Risikobewertung (Amazon Web Services)

A. Sachverhalt

Der Auftragnehmer nutzt Amazon Bedrock für die KI-gestützte Analyse und Amazon SES für den E-Mail-Versand. Vertragspartner ist Amazon Web Services EMEA SARL (Luxemburg). Die Verarbeitung erfolgt ausschließlich in AWS-Regionen innerhalb der EU. Amazon Web Services EMEA SARL ist eine Tochtergesellschaft der Amazon.com, Inc. (USA).

B. Rechtliche Einordnung

Im Standardbetrieb findet keine Übermittlung personenbezogener Daten in ein Drittland im Sinne von Kapitel V DSGVO statt. Es besteht jedoch ein potenzielles Risiko, dass US-Behörden auf Grundlage von US-Recht (insbesondere CLOUD Act und FISA 702) über die Konzernmutter Zugriff auf in der EU gespeicherte Daten verlangen. Zudem kann ein Fernzugriff durch AWS-Personal außerhalb der EU (etwa im Support-Fall) eine Übermittlung auslösen.

C. Bewertung des Risikos

- An AWS werden nur die für die jeweilige Prüfung erforderlichen Dokumentinhalte (Bedrock) beziehungsweise Empfängeradresse und Nachrichteninhalt (SES) übermittelt. Bedrock speichert Eingaben und Ausgaben nicht; SES speichert Nachrichten nur für die Dauer der Zustellung.
- Die verarbeiteten Daten sind Geschäftsdaten aus Leistungsverzeichnissen mit geringem Schutzbedarf für die betroffenen Personen (überwiegend berufliche Kontaktdaten von Projektbeteiligten). Besondere Kategorien werden nicht verarbeitet.
- Dem Auftragnehmer sind keine Fälle bekannt, in denen AWS Kundendaten aus EU-Regionen an US-Behörden herausgegeben hat; AWS verpflichtet sich vertraglich, Behördenanfragen zu prüfen, anzufechten und den Kunden zu informieren, soweit rechtlich zulässig, und veröffentlicht hierzu regelmäßige Transparenzberichte.

D. Absicherung

- AWS GDPR Data Processing Addendum als Bestandteil des AWS-Vertragswerks, einschließlich der Standardvertragsklauseln (EU) 2021/914 (Modul 3, Auftragsverarbeiter zu Auftragsverarbeiter).
- Amazon Web Services, Inc. ist nach dem EU-US Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795) zertifiziert; die Zertifizierung wird jährlich überprüft. Die Standardvertragsklauseln greifen automatisch, falls die Zertifizierung entfällt oder der Angemessenheitsbeschluss aufgehoben wird.
- Beschränkung der Verarbeitung auf AWS-Regionen innerhalb der EU durch technische Konfiguration (EU-Inferenzprofile, Region eu-central-1).
- Transportverschlüsselung aller Verbindungen zu AWS.
- Keine Nutzung von Eingaben und Ausgaben zum Training von Modellen und keine Weitergabe an Modellanbieter nach den Nutzungsbedingungen von AWS.

E. Ergebnis und Überprüfung

Unter Berücksichtigung der Art der Daten, der technischen Beschränkung auf EU-Regionen und der vertraglichen Garantien bewertet der Auftragnehmer das Restrisiko als gering. Der Einsatz von AWS ist datenschutzrechtlich zulässig. Der Auftragnehmer überprüft diese Bewertung mindestens jährlich, erstmals im September 2027, sowie anlassbezogen, insbesondere bei Wegfall der DPF-Zertifizierung von AWS, Aufhebung oder Änderung des Angemessenheitsbeschlusses durch den Gerichtshof der Europäischen Union oder die Europäische Kommission, wesentlichen Änderungen des AWS-Vertragswerks oder einem Wechsel der eingesetzten AWS-Dienste. Ergibt die Überprüfung ein erhöhtes Risiko, ergreift der Auftragnehmer zusätzliche Maßnahmen oder wechselt den Anbieter und informiert den Verantwortlichen nach § 5 Abs. 2.
