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.
