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).
