Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO:

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- Zutrittskontrolle
    - Server in Nürnberg
        - dokumentierte Schlüsselvergabe an Mitarbeiter
        - 24/7 personelle Besetzung der Rechenzentren
        - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Mitarbeiters
- Zugangskontrolle
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
    - Das Passwort zur Administrationsoberfläche wird vom Auftragnehmer selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen.
- Zugriffskontrolle
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
        - Die Verantwortung der Zugriffskontrolle obliegt dem Auftragnehmer.
        - Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.
- Datenträgerkontrolle
    - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
    - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum zerstört („geschreddert“).
- Trennungskontrolle
    - Daten des Auftraggebers werden logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt auf physisch getrennten Systemen.
- Pseudonymisierung
    - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
    - Alle Mitarbeiter sind i. S. d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
    - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
    - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

- Eingabekontrolle
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
    - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
    - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
    - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
    - Monitoring aller relevanten Server.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
    - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Incident-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- Auftragskontrolle
    - Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
    - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
    - Die Continux GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.