Anlage 2

zum Vertrag über eine Auftragsdatenverarbeitung nach Art. 28 DSGVO

vom xx.xx.xxxx

**Datenschutz-, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen**

1. Vertraulichkeit (Art. 32 lit. b DSGVO)
	1. **Zutrittskontrolle**

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

-

-

-

-

(z. B. Pförtner, Ausweisleser, kontrollierte Schlüsselvergabe, Werkschutz etc.)

* 1. **Zugangskontrolle**

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden:

-

-

(z. B. Login mit Benutzerkennung und Passwort, Bildschirmschoner mit Passwort-aufforderung)

* 1. **Zugriffskontrolle**

Maßnahmen, nach denen Berechtigte ausschließlich auf diejenigen Daten zugreifen können, die ihrer Zugriffsberechtigung unterliegen und nach denen personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

-

-

-

(z. B. Trennung von Test- und Produktiv-Daten, keine Vermischung mit Daten anderer Auftraggeber)

1. **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
	1. **Weitergabekontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

-

-

-

-

(z. B. Verschlüsselung/Tunnelverbindung (VPN), WLAN-Verschlüsselung, elektronische Signatur, Transportsicherung, Protokollierung).

* 1. **Eingabekontrolle**

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

-

-

-

-

(z. B. Logfile oder andere Protokollierungssysteme)

1. **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)**
	1. **Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können:

-

-

-

-

(z. B. regelmäßige Datensicherungen, Spiegeln von Festplatten (z. B. RAID), un-terbrechungsfreie Stromversorgung (USV), Einsatz von Virenschutz und Firewall)

1. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGV; Art. 32 Abs.1 lit d DSGVO)**
	1. **Datenschutz-Management**

Kurzbeschreibung des Datenschutzmanagementsystems, bspw. Definition von Rollen und Verantwortlichkeiten, Kontrollen und Überwachung der Wirksamkeit etc.

-

-

-

* 1. **Incident-Response Management**

Beschreibung etablierter Prozesse zum Umgang mit Sicherheitsvorfällen

-

-

-

* 1. **Datenschutzfreundliche Voreinstellungen (Art.25 Abs. 2 DSGVO)**

Maßnahmen zur Sicherstellung datenschutzfreundlicher Voreinstellungen (Grundsatz der Datenminimierung im Bereich Umfang der Daten, Speicherfrist, Zugänglichkeit)

-

-

-

* 1. **Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

-

-

-

(z. B. keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers eindeutige Vertragsgestaltung, sorgfältige Auswahl des Auftragnehmers, Kontrolle der Vertragsausführung)

1. **Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)**

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

-

-

-

1. **Vorlage für das Verzeichnis der Verarbeitungstätigkeiten**

Bitte hier die Verarbeitung gemäß Art. 30 DSGVO beschreiben oder als Anlage anfügen.