

**Das Formblatt ist nach Auftragserteilung ausgefüllt beim Auftraggeber einzureichen.**

**„Technisch-organisatorische Maßnahmen“ zu den Zusätzliche Vertragsbedingungen über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO**

Folgende besonderen technischen und organisatorischen Maßnahmen werden eingehalten.

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

- Zutrittskontrolle: Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren.  
☐ Schlüssel ☐ elektr. Türöffner ☐ Alarmanlagen ☐ Videoanlagen ☐ Pförtner
- Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.  
☐ Kennwörter ☐ autom. Sperrmechanismen ☐ Verschlüsselung von Datenträgern
- Zugriffskontrolle: Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.  
☐ Berechtigungskonzepte ☐ bedarfsgerechte Zugriffsrechte ☐ Protokollierung von Zugriffen
- Trennungskontrolle: Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. ☐ Mandantenfähigkeit ☐ Sandboxing
- Pseudonymisierung: Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer konkreten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

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

- Weitergabekontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten bei elektronischer 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.  
☐ Verschlüsselung ☐ Virtual Private Networks (VPS) ☐ elektr. Signatur
- Eingabekontrolle: Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind ☐ Protokollierung ☐ Dokumentenmanagement

### **3. Verfügbarkeit und Belastbarkeit**

- Verfügbarkeitskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.  
☐ Virenschutz ☐ Firewall ☐ Notfallpläne
- Belastbarkeit: Mindestmaßnahmen, die sicherstellen, dass im Falle eines Ausfalls der Datenverarbeitungssysteme diese rasch wiederhergestellt werden können.

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

- Datenschutz-Management
- Incident-Response-Management: Maßnahmen zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten, im Rahmen der Auftragsverarbeitung nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können