Anhang 1 „Technisch-organisatorische Maßnahmen“ ***Vom Bewerber zu ergänzen***

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbetriebliche Organisation des Auftragsverarbeiters
Der Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	*[**Vom Bewerber zu ergänzen**] z.B. Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung*
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	*[**Vom Bewerber zu ergänzen**] z.B. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Kennwortverfahren, Automatisches Sperren, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern)*

3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	*[**Vom Bewerber zu ergänzen**] z.B. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung)*
4.	**Weitergabekontrolle** Es ist zu 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.	*[**Vom Bewerber zu ergänzen**] z.B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur*
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	*[**Vom Bewerber zu ergänzen**] z.B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Auswertungssysteme*

6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	*[**Vom Bewerber zu ergänzen**] Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragsverarbeiters, Kontrolle der Vertragsausführung)*
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	*[**Vom Bewerber zu ergänzen**] z.B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung (Beispiel: Backup-Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan)*
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	*[**Vom Bewerber zu ergänzen**] z.B. Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion / Test*

Anhang 2 — Unterauftragsverhältnisse ***Vom Bewerber zu ergänzen, falls einschlägig***

Der Auftragsverarbeiter setzt bei der Verarbeitung personenbezogener Daten für den Verantwortlichen die folgenden Subunternehmer mit dem jeweils beschriebenen Auftragsinhalt ein. Der Verantwortliche ist mit diesem Einsatz der Subunternehmer einverstanden.

Subunternehmer	Auftragsinhalt
Vom Bewerber zu ergänzen, falls einschlägig	***Vom Bewerber zu ergänzen***