## Anlage 7

# Technische und organisatorische Maßnahmen

Die Anlage beschreibt die technischen und organisatorischen Maßnahmen die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung gem. Art. 24 DS-GVO erfolgt. Diese ergeben sich aus Art. 32 Abs. 1 DS-GVO. Der Auftragnehmer hat nachfolgende Maßnahmen hierzu umgesetzt.

| Schutzziele | Maßnahme | Umsetzung der Maßnahme |
|---|---|---|
| **Vertraulichkeit**<br><br>Art. 32 Abs. 1 lit. b) DS-GVO | **Zutrittskontrolle**<br><br>Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. | • Ausgabe von Besucher-/Mitarbeiterausweisen<br>*(Es gilt diese an Gegebenheiten des Auftragsnehmers anzupassen)* |
| | **Zugangskontrolle**<br><br>Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. | • Festlegung befugter Personen<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| | **Zugriffskontrolle**<br><br>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. | • Aufgabenverteilung<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| | **Trennungskontrolle**<br><br>Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. | • Funktionstrennung und Verfahrensdokumentation<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |

| | | |
|---|---|---|
| **Integrität**<br><br>Art. 32 Abs. 1 lit. b) DS-GVO | **Weitergabekontrolle**<br><br>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 personen-bezogener Daten durch Einrichtungen zur Daten-übertragung vorgesehen ist. | • Dokumentation der Abruf- und Übermittlungsprogramme sowie zu den Stellen, an die eine Übermittlung vorgesehen ist<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| | **Eingabekontrolle**<br><br>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. | • Protokollierung der Eingaben<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| **Verfügbarkeit und Belastbarkeit**<br><br>Art. 32 Abs. 1 lit. b) DS-GVO | **Verfügbarkeitskontrolle**<br><br>Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | • Konzept zur Durchführung von regelmäßigen Datensicherungen<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| **Wiederherstellbarkeit**<br><br>Art. 32 Abs. 1 lit. c) DS-GVO | **Maßnahmen zur raschen Wiederherstellbarkeit**<br><br>Bei einem unvorhergesehenen Zwischenfall ist dafür zu sorgen, dass die personenbezogenen Daten „rasch“ ihrem Zweck entsprechend wieder genutzt werden können. | • Spiegelung der Daten an zwei Standorten<br>• Konzept zur Sicherung der Datenbestände<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |

| | | |
|---|---|---|
| **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**<br><br>Art. 32 Abs. 1 lit. d) DS-GVO | **Auftragskontrolle**<br><br>Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. | • Sorgfältige Auswahl der Auftragnehmer<br>• Dokumentation von kundenbezogenen Anweisungen<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| | **Datenschutz-Management**<br><br>Zum Schutz personenbezogener Daten ist sicherzustellen, dass eine Datenschutzorganisation etabliert ist und Verantwortlichkeiten festgelegt sind. | • Regelungen zum Datenschutz-Management<br>• Verzeichnisse von Verarbeitungstätigkeiten<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| **Pseudonymisierung und Verschlüsselung**<br><br>Art. 32 Abs. 1 lit. a) DS-GVO | **Pseudonymisierung**<br><br>Die Gestaltung der Datenverarbeitung hat eine Minimierung von Risiken betroffener Personen zu gewährleisten. | • Ersetzen von Identifikationsmerkmalen durch Ordnungsziffern oder sonstige Kennzeichen<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |
| | **Verschlüsselung**<br><br>Zugang zu den personenbezogenen Daten ist ausschließlich dem befugten Personenkreis zu gewähren. | • Angemessene Verschlüsselung nach Stand der Technik<br>*(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)* |

Es handelt sich bei den beschriebenen technischen und organisatorischen Maßnahmen um keine abschließende Auflistung. Diese und **weitere** Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der in dieser Anlage beschriebenen Schutzziele. Weiterhin unterliegen die Maßnahmen dem technischen Fortschritt und der Weiterentwicklung. Dabei wird das tatsächliche Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten.