Anlage 2 zum AVV nach Art. 28 DSGVO:
Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat.

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

Getroffene Maßnahmen:

- ⊗ Transportverschlüsselung bei Fernwartungszugriffen
- ⊗ Festplattenverschlüsselung auf den Administrator Laptops oder PCs
- ⊗ Verwendung von VPN und Proxy Systemen

B. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1. Zutrittskontrolle

Gewährleistung, dass der Zutritt zu den Betriebsarealen und deren Bereichen nur berechtigten Personen möglich sind: Der Zutritt ist über eine Zentralschließanlage geregelt. Innerhalb des Gebäudes ist jede Etage durch eine weitere Sicherheitstüre gesichert.

Getroffene Maßnahmen:

- ⊗ Rechenzentrum mit ausreichender Zugriffskontrolle.

2. Zugangskontrolle

Gewährleistung, dass nur Mitarbeiter der verantwortlichen Stelle oder Arbeitskräfte, die im Rahmen einer Auftragsverarbeitung verpflichtet sind, in den hierfür vorgesehenen Aufgabenbereich dürfen und mit Benutzeridentifikation entsprechende Daten verarbeiten:

Getroffene Maßnahmen:

- ⊗ Wartungsarbeiten an der interner IT und Servern bedürfen unserer ausdrücklichen Zustimmung. Sie dürfen nur begonnen werden, wenn sich das Wartungspersonal mit Benutzerkennung und Passwort angemeldet hat.

3. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugriff haben:

Getroffene Maßnahmen:

- ⊗ Unseren Auftragnehmern werden nur die Zugriffsrechte eingeräumt, die diese zur Durchführung der Wartungsarbeiten tatsächlich benötigen.
- ⊗ Eine Reihe von Hardware- und Softwareidentifikationsmaßnahmen, die Verschlüsselung der Daten bei der Datenübertragung sowie ein mehrstufiges

Zugriffs- und Nutzungskontrollverfahren schließen den unbefugten Zugriff auf die gespeicherten Datenbestände und die unberechtigte Kenntnisnahme aus.

- ⊗ Es wird sichergestellt, dass das IT-Personal nur insoweit auf gespeicherte personenbezogene Daten zugreifen kann, als dies zur Durchführung von Wartungsarbeiten unerlässlich notwendig ist.

4. Benutzerkontrolle

Gewährleistung der Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

Getroffene Maßnahmen:

- ⊗ Einsatz eines Berechtigungskonzepts in File Server und Anwendungen die ein Berechtigungskonzept ermöglichen

5. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten. Die Plausibilisierung der Dateneingabe findet dabei auf revisionsrelevanten Feldern statt und wird entsprechend der zugehörigen Prozesse validiert.

Getroffene Maßnahmen:

- ⊗ Protokollierung der Systemnutzung und Auswertung der Protokollierung

6. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung; das heißt, alle in die Datenverarbeitung eingebundenen Abteilungen sind funktionell, organisatorisch getrennt. Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zu Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist.

Getroffene Maßnahmen:

- ⊗ Schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zu Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist.
- ⊗ In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung.
- ⊗ Trennung von Produktiv- und Testsystemen sowie Ordnerstrukturen und Datenbanken

C. Integrität (Art. 32 Abs. 1 lit. c) DSGVO)

7. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können:

Getroffene Maßnahmen:

- ⊗ Softwareseitiger Ausschluss durch Mandantentrennung und/oder Datei-Separierung.
- ⊗ Je nach Dienstleistung hardwareseitiger Ausschluss durch dedizierte Server Ressourcen.

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen von Weisungen verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben. Strenge Richtlinien und Arbeitsanweisungen beim Auftragnehmer gewährleisten, dass eine unbefugte Weitergabe oder das Entfernen von Daten verhindert wird. Entsorgungsgut mit schutzwürdigem Inhalt wird unter Beachtung der Sicherheitsstufen des Grades der Vernichtung nach DIN 66399 vernichtet.

Getroffene Maßnahmen:

- ⊗ Daten werden nur in verschlüsselter Form übermittelt (Transportverschlüsselung bei Fernwartungszugriffen).
- ⊗ Für Wartungen und Zugriffe auf Daten wird ein VPN eingesetzt.
- ⊗ Festplatten sind per GPO verschlüsselt.

9. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Getroffene Maßnahmen:

- ⊗ Protokollierung der Datenübermittlungsstelle/-wege, welche im Verdachtsfall ausgewertet werden können
- ⊗ Die technische Absicherung erfolgt über Firewall und Proxysysteme

10. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind:

Alle anfallenden personenbezogenen Daten werden nur entsprechend den jeweils geltenden Vorschriften zum Schutz personenbezogener Daten, nur zum Zwecke der jeweiligen Auftragsabwicklung sowie zur Wahrung berechtigter eigener Geschäftsinteressen im Hinblick auf die Beratung und Betreuung von Kunden und zur Abwicklung der arbeitsvertraglichen Grundlagen verarbeitet.

Getroffene Maßnahmen:

- ⊗ Protokollierung der Systemnutzung und Auswertung der Protokollierung

- ⊗ Durchführung von Schulungsmaßnahmen für die Softwarenutzung
- ⊗ Alle Mitarbeiter werden in regelmäßigen Abständen zum Datenschutz geschult

11. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Getroffene Maßnahmen:

- ⊗ Ereignisprotokollierung der Systeme mit Meldung von Störungen
- ⊗ Wartungsverträge und SLA-Vereinbarungen garantieren die Zuverlässigkeit unserer Systeme
- ⊗ Zertifiziertes Rechenzentrum als Hoster (24x7)

12. Auftragskontrolle

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

Der Weisungsrahmen ist durch einen schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag unter Berücksichtigung der gesetzlichen Pflichtinhalte sowie ferner durch die Anwendungsbeschreibung der Dienstleistung eindeutig vorgegeben. Gleiches gilt für auftragsbezogene Auskünfte; sie werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt, Ausnahmen vom konkreten Weisungsrahmen gelten für technisch bedingte Verarbeitungen, z. B. für die interne Datensicherung. Auftragnehmer dürfen von den ihnen zur Durchführung eingeräumten Rechten nur in dem für die Durchführung unerlässlich notwendigen Umfang Gebrauch machen.

Getroffene Maßnahmen:

- ⊗ Alle Dienstleister, welche die Möglichkeit haben, personenbezogene Daten einzusehen, werden auf das Datengeheimnis und zur Zweckbindung bei einer Auftragsverarbeitung verpflichtet
- ⊗ Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben
- ⊗ Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag unter Berücksichtigung der Pflichtinhalte sowie ferner durch die Anwendungsbeschreibung der Dienstleistung eindeutig vorgegeben.
- ⊗ Auftragsbezogene Auskünfte werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt; Ausnahmen vom konkreten Weisungsrahmen gelten nur für technisch bedingte Verarbeitungen, z. B. zur internen Sicherung

D. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. c) DSGVO)

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

Ein mehrstufiges Protokollverfahren gewährleistet soweit möglich, dass keine Datenveränderungen unbemerkt vorgenommen werden können. Protokolliert wird sowohl auf

Client als auch serverseitig. Schwerpunkt der Protokollierung liegt dabei auf Anwendungs-, System- und Sicherheitsebene.

Getroffene Maßnahmen:

- ⊗ Zertifiziertes Rechenzentrum als Hoster (24x7)

14. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:

Zahlreiche Datensicherungsmaßnahmen gewährleisten, dass personenbezogene und andere schutzwürdige Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Getroffene Maßnahmen:

- ⊗ Es bestehen Notfall- und Wiederherstellungspläne für alle wichtigen Systeme.
- ⊗ Sicherungen werden nach einem definierten Backup-Plan täglich und wöchentlich durchgeführt.
- ⊗ Einsatz von Raid-Systemen sowie Spiegelung der Datenbestände

E. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. c) DSGVO)

Getroffene Maßnahmen:

- ⊗ Regelmäßige Überprüfung der Verarbeitungsverzeichnisse und der technischen und organisatorischen Maßnahmen sowie bei Bedarf

Stand: 6. Februar 2023

-- Ende Anlage 2 --