Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Büroumgebung
  - Für die Außen- und Innensicherung sind innerhalb und außerhalb der Arbeitszeiten folgende - Maßnahmen zur Zutrittskontrolle getroffen:
    - Dritten / Unbefugten wird der Zutritt zu Systemen verwehrt
    - Festlegung befugter Personen, Schlüsselregelungen
    - Einbruchmeldeanlagen
    - Abholung und Begleitung von Besuchern

  Internes Rechenzentrum
  - Der Zutritt ist nur ausgewiesenen Mitarbeitern möglich. Das interne Rechenzentrum genügt den Ansprüchen und werden regelmäßig überprüft.

  Externe Rechenzentren
  - Der Zutritt ist nur ausgewiesenen Mitarbeitern möglich. Die externen Rechenzentren genügen den Ansprüchen und werden regelmäßig überprüft.

- Zugangskontrolle
  Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, können nicht von Unbefugten genutzt werden. Es wird gewährleistet, dass nur autorisierte Mitarbeiter Zugang zu den verarbeiteten Daten haben. Hierfür werden folgende Sicherungsmaßnahmen verwendet:
  - Eindeutige Identifizierung des Nutzers gegenüber dem System
  - Festgelegte Berechtigungsstrukturen
  - Arbeitsanweisung zur Bildschirmsperre
  - Technische Prüfung der Passwortqualität
  - Einsatz einer Firewall

- Zugriffskontrolle
  Es wird gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

  Maßnahmen zur Sicherstellung der Zugriffskontrolle:
  - Restriktive differenzierte Rechtevergabe
  - Es wird KEIN Modemzugriff eingesetzt, nur reine LAN / IP / VPN Kommunikation
  - Die Remote Zugänge sind verschlüsselt und so gering wie möglich gehalten in der Anzahl.
  - Es existiert eine Passwortrichtlinie.
  - Es existieren Testsysteme.
  - Datenterminals werden bei Nichtbenutzung gesperrt.

- Trennungskontrolle
  Daten sind logisch im Rahmen der Zugriffskontrolle getrennt. Durch die Trennung können jederzeit Daten auf Anforderung des Partners vollständig gelöscht werden.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Eine Pseudonymisierung findet nicht statt.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
- Weitergabekontrolle
  Werden Daten an Dritte weitergegeben im Sinne der Auftragsdatenverarbeitung, dann gilt:
  - Es erfolgt eine Verschlüsselung der Datenträger.
  - Es erfolgt der Transport per Kurier oder Einschreiben
  - Es wird in jedem Fall ein Transportbegleitschein beigefügt, der nach Rücksendung in ein Protokollbuch eingetragen wird.
  - Es werden die Datenträger als Datenträger des Mandanten gekennzeichnet.
  - Alte Datenträger werden kontrolliert vernichtet durch einen Entsorger inkl. Protokoll.
  - Alle Datenträger werden verschlossen aufbewahrt.
  - Nur festgelegte Mitarbeiter haben Zugang zu den Datenträgern.

- Eingabekontrolle
  Durch Protokollierung wird festgestellt, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
- Verfügbarkeitskontrolle
  Es wird sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.
  - Brandschutzmaßnahmen
  - Überspannungsschutz
  - Unterbrechungsfreie Stromversorgung
  - Klimaanlage
  - RAID (Festplattenspiegelung)
  - Backupkonzept
  - Virenschutzkonzept
  - Schutz vor Diebstahl

- Durch ein Backup und Desaster Recovery Konzept wir die rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) sichergestellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
- Vorhandenes Datenschutz-Management System
- Vorhandenes Incident-Response-Management über das eingesetzte Ticket-System
- Regelmäßige Datenschutzaudits durch den Datenschutzbeauftragten
- Auftragskontrolle
  Schriftliche Verträge zwischen dem Auftraggeber und dem Auftragnehmer (Vertrag zur Auftragsdatenverarbeitung gemäß § 11 BDSG) unter anderem zur Fixierung der Weisungen und Berichtspflichten sowie sorgfältige Auswahl des Auftragnehmers nach dem Niveau seiner technischen und organisatorischen Maßnahmen.