Anlage 1 – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen
  - Sicherung durch Bewegungsmelder und Kamera
  - Zutritt für Besucher ist nur über Hauseingangs- & Bürotür möglich
  - Abgeschlossener Serverraum.
- Zugangskontrolle
  Keine unbefugte Systembenutzung
  - Anti-Viren-Software, sowie Crypto-Trojaner-Schutz auf Servern & Clients
  - Verschlüsselung lokaler Datenträger der Server, Clients & Backups
  - Authentifizierung zum Netzwerk und zur Software mit Benutzername & Passwort
  - Personenbezogene Benutzerprofile und Gruppenberechtigungen
  - Hardware-Firewall wird eingesetzt
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
  - Sorgfältig ausgewählte Mitarbeiter und Verpflichtung zur Einhaltung der Vertraulichkeit
  - Rechteverwaltung durch Systemadministrator
  - Passwortrichtlinie für Benutzer wurde erstellt
  - Berechtigungen und bedarfsgerechte Zugriffsrechte zum Schutz der Daten sind vorhanden
  - Differenzierung und Trennung administrativer und weiterer Arbeiten auf dem System sind gewährleistet
  - Datenträger werden sicher aufbewahrt und nach Gebrauch ordnungsgemäß vernichtet
  - Regelmäßige Backups der Software und Daten
  - Vernichtung personenbezogener Daten in Papierform durch einen Aktenvernichter
- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden,
  - Mandantentrennung möglich, falls erforderlich
  - Funktionstrennung möglich, falls erforderlich
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen 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 DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
  - Verschlüsselte E-Mail-Übertragung (SSL/TLS)
  - Datentransfer via Teamviewer mit Verbindungsprotokoll
  - Übertragung von Daten per VPN
- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
  - Protokollierung von Netzwerkan und -abmeldungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b,c DS-GVO)

- Verfügbarkeits- & Belastbarkeitskontrolle & rasche Wiederherstellbarkeit
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
    - Alarmmeldung bei unberechtigten Zutritt in Serverräumen
    - Feuer- und Rauchmeldeanlagen, Feuerlöschgeräte in Serverräumen
    - Unterbrechungsfreie Stromversorgung mit Überspannungsschutz
    - Datenspeicherung erfolgt Serverseitig
    - RAID-Systeme für produktives System und Backup-System
    - Tägliche Daten-Backups (Vollsicherung) mit Übertragung an einen anderen sicheren Ort auf ein verschlüsseltes Backup-Medium, sowie regelmäßige Image-Sicherung der Server
    - Serverräume: keine Wasserrohre, Abwasser- oder Gasleitungen

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);