Anlage – Technisch-organisatorische Maßnahmen (Nachfolgende Maßnahmen sind bei der TEHA GmbH implementiert)

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

- **Zutrittskontrolle**
  - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch elektrische Türöffner und Empfangsdame
  - Sicherheitsschlösser
  - Dokumentierte Schlüsselregelung
  - Sorgfältige Auswahl von Reinigungspersonal

- **Zugangskontrolle durch**
  - Keine unbefugte Systembenutzung durch Implementierung von sicheren Kennwörtern
  - Automatische Sperrmechanismen
  - Verschlüsselung bzw. Sperrung von USB Prots
  - Zuordnung von Benutzerrechten
  - Erstellen von Benutzerprofilen
  - Zuordnung von Benutzerprofilen zu IT-Systemen
  - Einsatz von Anti-Viren-Software
  - Einsatz einer Hardware-Firewall

- **Zugriffskontrolle durch**
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Implementierung eines Berechtigungskonzeptes und bedarfsgerechten Zugriffsrechten
  - Protokollierung von Zugriffen
  - Erstellen eines Berechtigungskonzepts
  - Verwaltung der Rechte durch Systemadministrator
  - Anzahl der Administratoren auf das „Notwendigste“ reduziert
  - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
  - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - Sichere Aufbewahrung von Datenträgern

- **Trennungskontrolle durch**
  - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
  - Logische Mandantentrennung (softwareseitig)
  - Erstellung eines Berechtigungskonzepts
  - Festlegung von Datenbankrechten

- Trennung von Produktiv- und Testsystem

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

- **Weitergabekontrolle durch**
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
  - Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
  - Eingabekontrolle
  - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

- **Verfügbarkeitskontrolle durch**
  - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie (online/offline; on-site/off-site), Virenschutz, Firewall, Meldewege und Notfallpläne;
  - Rasche Wiederherstellbarkeit durch tägliche Datenübertragung (Art. 32 Abs. 1 lit. c DS-GVO);
  - Feuer- und Rauchmeldeanlagen
  - Feuerlöschgeräte in Serverräumen
  - Erstellen eines Backup- & Recoverykonzepts
  - Testen von Datenwiederherstellung
  - Erstellen eines Notfallplans
  - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
  - Serverräume nicht unter sanitären Anlagen

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

- Incident-Response-Management (IT Störungsmanagement);
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers (Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Nachkontrollen)
- Protokollierung von Eingabe, Änderung, Löschung von Daten
- Löschbarkeit von Daten

Auftragskontrolle durch

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten

- Schriftliche Weisungen an den Auftragnehmer durch eine Auftragsdatenverarbeitungsvertrag
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer in der ADV vereinbart
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG) Ab 25.05.2018 Datengemeinmis nach §53 Bundesdatenschutzgesetz
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten