Technische und Organisatorische Maßnahmen
Nach Art. 32 Datenschutz-Grundverordnung (DSGVO)

1. **Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**
   a. **Zutrittskontrolle**

   Der unbefugte räumliche Zutritt ist zu verhindern.

   - Gelände
     - Das Betriebsgelände liegt in einem Wohngebiet
     - Das Betriebsgelände ist eingezäunt
   - Gebäude & Fenster
     - Die Gebäudetüren sind einbruchhemmend
     - Die Gebäudefenster sind einbruchhemmend
     - Die Fenster befinden sich oberhalb des Erdgeschosses
   - Räume
     - Büro ist abschließbar
     - Serverraum ist abschließbar

   b. **Zugangskontrolle**

   Das Eindringen in die Datenverarbeitungssysteme ist zu verhindern.

   - Benutzeranmeldung
     - Jeder Anwender hat einen eigenen Benutzernamen und ein eigenes Passwort
   - Passwortkonventionen
     - Sperrung bei wiederholter Fehleingabe
     - Festgelegte Mindestlänge
     - Ausschluss von Trivialpasswörtern
     - Änderung bei der ersten Anmeldung
     - Kontrolle der Passwortkonventionen
     - Verwendung von Sonderzeichen
   - Bildschirmschoner
     - Automatische Aktivierung des Bildschirmschoners
     - Deaktivierung des Bildschirmschoners nur mit Passwort möglich
   - Firewall
     - Das LAN ist mit einer Firewall gegen das Internet abgeschottet
   - Anti-Viren-Konzept
     - Jeder Rechner (Server, PC, Laptop, Stand-Alone, etc.) ist mit einem Anti-Viren-Programm ausgestattet
     - Automatisches Update der Anti-Viren-Signaturen
     - Zentrale Administration der Anti-Viren-Programme
   - Sicherheits- / Programmupdates
     - Regelmäßiges (teils automatisches) Einspielen von Sicherheitsupdates
     - Regelmäßiges (teils automatisches) Einspielen von Programmupdates
   - WLAN-Nutzung
     - Nutzung von WPA2/WPA3
     - Passwortvergabe unterliegt den Passwortkonventionen
   - Fernwartung
     - Fernwartung wird genutzt
     - Übertragung erfolgt verschlüsselt
     - Verträge gemäß DSGVO mit externen Dienstleistern liegen vor und können eingesehen werden

   c. **Zugriffskontrolle**

   Mit einem Berechtigungskonzept sind unerlaubte Tätigkeiten in den Datenverarbeitungssystemen zu verhindern.

- Berechtigungskonzept
  - Systemtechnische Vergabe von Berechtigungen
  - Rollenberechtigungen werden vergeben
  - Gruppenberechtigungen werden vergeben
  - Es erfolgt eine Kontrolle der Berechtigungen
  - Es gibt ein Verfahren zum Entzug von Berechtigungen
- Systemadministration
  - Die Administration der IT-Systeme erfolgt intern

d. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Trennung der Interessenten und Kunden durch Software
- Logische Trennung der Daten
- Trennung über Zugriffsregelungen
- Trennung von Test- und Produktionsdaten

e. Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

Maßnahmen, die gewährleisten, dass Datenschutzgrundsätze, wie etwa Datenminimierung wirksam umgesetzt werden und die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen dieser Verordnung zu genügen.

- Es werden geeignete technische organisatorische Maßnahmen zur Aufbewahrung der Zuordnungsdaten ergriffen
- Wo möglich und notwendig werden personenbezogene Daten verschlüsselt
- Data Masking der Authentifizierungsdaten (Passwort-Hashing)
- Die Pseudonymisierung ist im Verarbeitungssystem so früh wie möglich durchzuführen
- Die Pseudonymisierung wird zum Schutz der Vertraulichkeit, wann immer möglich, praktiziert

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a. Weitergabekontrolle

Die Weitergabe (elektronische Übertragung, Datentransport, Übermittlungskontrolle, etc.) personenbezogener Daten ist zu regeln.

- Datenträger
  - Datenbestände auf externen Datenträgern sind verschlüsselt
  - Explizites Verbot zur Nutzung privater Speichermedien
- Datenträgervernichtung
  - Vernichtung von Papierdokumenten mittels Aktenvernichter (Sicherheitsstufe 3)
- Weitergabe von personenbezogenen Daten
  - Weitergabe von Daten per Internet, E-Mail, E-Mail mit verschlüsseltem Dateianhang
  - Netzwerklaufwerk
  - Nutzung von VPN
  - Weitergabe von Daten per Briefpost
- Cloud-Services
  - Es werden keine Cloud-Services genutzt
- Fernwartung durch Externe
  - Es werden keine Externen zur Prüfung und / oder Wartung herangezogen

b. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege.

- Verwendung personalisierter Logins
- Protokollierung von Operationen und Zugriffen im Fermennetzwerk

3. Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) und Desaster Recovery (Art. 32 Abs. 1 lit. c DSGVO)

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Serverraum

- Brandschutzmaßnahmen (Feuerlöscher)
- Feuer- und Rauchmelder installiert
- Separate Absicherung des Stromkreises

- Datensicherungskonzept
  - Die Daten werden gemäß eines noch nicht protokollierten Sicherungskonzepts gesichert
- IT-Redundanzen
  - Systeme sind redundant ausgelegt
- Virtualisierung
  - Server / Dienste sind teils virtualisiert
  - Die virtualisierten Server / Dienste sind im Datensicherungskonzept eingebunden
- Systempasswörter
  - Systempasswörter sind für den Notfall sicher hinterlegt
- Desaster Recovery
  - Notfallplan
  - Datensicherungskonzepte und Umsetzung
  - Im Rahmen des Serverbetrieb erstellt die STRATO AG täglich ein Vollbackup des gesamten Servers, welches durch Bettysoft zu jeder Zeit wiederhergestellt werden kann

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

a. Datenschutz-Management

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

- Regelmäßige Schulungen der Mitarbeiter:innen zum Datenschutz
- Ein VVT ist vorhanden, vollständig und aktuell
- Die Aufbewahrung der elektronischen Protokolle ist geregelt
- Es gibt Regelungen für die Sicherung des Datenbestandes
- Verschiegenheitserklärungen nach DSGVO der Mitarbeiter:innen sind vorhanden
- Ein Datenschutzkonzept ist vorhanden
- Sofern erforderlich werden Datenschtuz-Folgeabschätzungen durchgeführt und protokolliert
- Protokoll- und Logdateien werden anlassbezogen ausgewertet
- Datenschutz- und Datensicherungsmaßnahmen werden gelegentlich unvermutet kontrolliert
- Transparenzpflichten werden eingehalten
- Accountabilität wird beachtet

b. Incident-Response-Management

Maßnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an den Auftraggeber erfolgt.

- Schulung der Mitarbeiter:innen bzgl. des Erkennens einer Datenpanne
- Ein nicht protokolliertes Konzept zur Meldung von Datenpannen an den Auftraggeber ist vorhanden
- Ein nicht protokolliertes, internes Incedent-Responce-Management-Konzept existiert

c. Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Privacy by Design wird beachtet
- Privacy by Default ist eingestellt

d. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit Bettysoft
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern