TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

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

a. Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Sämtliche Zugänge sind ausreichend gegen den unbefugten Zutritt abgesichert.

- Schlüsselvergabe erfolgt nur an ausgewählte vertrauenswürdige Personen
- die den Mitarbeitern zur Verfügung gestellten Schlüssel werden personengebunden registriert sowie die Schlüsselausgabe quittiert wird;
- Räume werden außerhalb der Dienstzeiten durch Videoüberwachung gesichert
- der Zugang zu Serverräumen wird nur einer begrenzten Anzahl von Personen gestattet;
- Türen sind mit einem manuellen Schließsystem versehen und werden grundsätzlich verschlossen sind;
- Besucher dürfen sich nur in Begleitung eines Mitarbeiters in den Räumlichkeiten bewegen;
- Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben wird sorgfältig ausgewählt.

b. Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

- alle technischen Systeme (zentral und dezentral), Hardware und Software Firewall geschützt sind;
- Mitarbeiter ausschließlich mit den personalisiert angelegten Benutzerprofilen arbeiten, welche die Eingabe eines spätestens aller drei Monate zu ändernden und mindestens 8 Stellen umfassenden alphanumerischen Passwort erfordern;
- Bildschirme automatisiert spätestens nach 3 Minuten sowie Zugänge bei mehr als drei Fehlversuchen gesperrt werden;

- VPN-Technologie (SSL/TLS) eingesetzt wird;
- mobile Datenträger (Laptops und Smartphones) gesondert verschlüsselt sind.

c. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

- systemimmanente Sicherungsmechanismen: differenzierte Berechtigungsvergabe je nach Aufgabe
- Prüfung der Zugriffsberechtigung: Durchführung regelmäßiger Stichproben für die unterschiedlichen Systeme
- Protokollierung der Zugriffe
- Alle Zugänge sind zusätzlich (sofern möglich) mit einer 2-Faktor-Authentifizierung geschützt (Yubikey, Google-Authenticator oder SMS)

d. Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- "Interne Mandantenfähigkeit" / Zweckbindung
- Datenstruktur-Konzept
- an Aufgaben orientierte Zugriffsverwaltung
- Trennung von Test- und Produktionsdaten
- Mandantenfähigkeit der Systeme

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

a. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Verfahren zur Identifizierung und Authentifizierung:
  - Mitarbeiter arbeiten ausschließlich mit den personalisiert angelegten Benutzerprofilen, die die Eingabe eines spätestens aller drei Monate zu ändernden und mindestens 8 Stellen umfassenden alphanumerischen Passwort erfordern;
  - Alle Zugänge sind zusätzlich (sofern möglich) mit einer 2-Faktor-Authentifizierung geschützt (Yubikey, Google-Authenticator oder SMS)

- Einsatz folgender Verschlüsselungs- und Hashing-Algorithmen
  - AES256,
  - BCrypt,
  - SCrypt,
  - Ed25519,
  - HMAC-SHA256,
  - HMAC-SHA512,
  - RSA mind. 2048 Bits,
  - Diffie-Hellman mind. 3072 Bits
- https (TLS 1.2 und höher)
- PGP

- Dokumentation von Datenempfänger und Transportwegen:
  - API Zugriffe auf das plenigo System werden gelogged
  - Daten werden nur verschlüsselt gespeichert
  - Audit-Logging innerhalb des plenigo-Systems
  - Regelung zur Fernwartung: je nach System individuell geregelt
  - Zugriff nur über VPN (wireguard und OpenVPN)

b. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

- Regelung von Zugriffsrechten
- Protokollierung von Zugriffen
- Regelung zu Aufbewahrung, Zugriff und Löschung der Protokolle beim Auftragnehmer

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

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- Maßnahmen zur Datensicherung (physikalisch / logisch):
  - Backup-Verfahren
  - Spiegeln von Festplatten, z.B. RAID-Verfahren
  - Sicherungs- und Wiederanlauf-Verfahren für Datenbestände und Systeme
  - Sicherungsrhythmen, Aufbewahrungszeit und Aufbewahrungsort für Back-up-Kopien

- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Firewall
- der vorhandene Virenschutz (Anti-Viren-Software) wird ständig gepflegt und aktualisiert
- Freigabeverfahren für neue IT-Verfahren: geregelt über IT Projektabläufe (Pflichtenheft, Abnahmeprotokolle, Test- und Produktivdatentrennung)
- Notfallplan

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

a. Datenschutz-Management

Das Datenschutzmanagement ist mit Hilfe einer Kombination aus Seafile und Confluence realisiert.

b. Incident-Response-Management

Notfallreaktions- und Bereitschaftsplan liegt allen wichtigen Stellen vor (Datenschutzbeauftragter, IT-Mitarbeiter). Etwaige Vorfälle werden im Support-Tool behandelt, gespeichert und können jederzeit nachvollzogen werden.

5. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Es werden nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind verarbeitet. Die von plenigo erfassten Daten können durch den Auftraggeber jederzeit im plenigo - Backend geändert werden.

6. **Auftragskontrolle Art. 28 DS-GVO**

Keine Auftragsverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung