Technische und organisatorische Maßnahmen gemäß DSGVO

I. Vertraulichkeit (Art. 32 Abs. 1 lit. a + b DSGVO)

1. **Zutrittskontrolle zu Verarbeitungsbereichen (Physischer Zugang)**
   - Aufrechterhaltung eines physischen Sicherheitskonzepts für die relevanten Standorte, einschließlich physischer Sicherheitszonen
   - Sicherstellung angemessener Zutrittskontrollmaßnahmen zu Gebäuden und Bereichen, die sich in verschiedenen physischen Sicherheitszonen befinden
   - Beschränkung des physischen Zutritts auf das erforderliche Minimum (Prinzip der geringsten Berechtigung)
   - Sicherstellung des physischen Schutzes von Perimeter, Gebäuden und Räumen durch Zäune, gesicherte Türen und Fenster
   - Verwaltung von Schlüsseln und Zutrittskarten
   - Beschränkung des Zutritts zu Serverräumen auf eine stark eingeschränkte Gruppe autorisierter Personen, einschließlich Maßnahmen zur Einbruchserkennung
   - Verwaltung von Besuchern an den Standorten
2. **Zugangskontrolle auf Datenverarbeitungssysteme (Authentifizierung)**
   - Sicherstellung einer starken Benutzerauthentifizierung (MFA) für das operative Personal, das an der Anwendung arbeitet
   - Authentifizierung technischer Benutzer mittels sicherer Authentifizierungsprotokolle
   - Sicherstellung der Netzwerkauthentifizierung zwischen Systemen oder Systemkomponenten mittels eines Maschinen-Zertifikats (Schnittstellen)
   - Authentifizierung anderer Anwendungen unter Verwendung technischer Benutzer mittels sicherer Authentifizierungsprotokolle
   - Sicherstellung der Einhaltung der Prinzipien "Clear-Screen", "Clean-Desk" und "Clean-Wall" an den Standorten und durch Personen im Geltungsbereich der Datenverarbeitungsdienste
   - Sicherstellung einer DMZ und eines Application Gateway für den Zugriff aus externen Netzwerken (z. B. dem Internet)
   - Implementierung von Malware-Schutz (einschließlich EDR auf Clients und Servern)
3. **Zugriffskontrolle zur Nutzung bestimmter Bereiche von Datenverarbeitungssystemen (Autorisierung)**

- Dokumentation des Rollen- und Berechtigungskonzepts
- Beschränkung des Zugriffs auf das erforderliche Minimum (Prinzip der geringsten Berechtigung)
- Verwendung personalisierter Benutzerkonten für das operative Personal, das an der Anwendung arbeitet
- Verhinderung des Zugriffs auf die Anwendung über Standard- oder Testkonten
- Verwendung eines Prozesses zur regelmäßigen Überprüfung und zum Entzug von Berechtigungen
- Erstellung separater Administratorkonten zur Verwaltung von Systemen
- Sicherstellung, dass Informationen (sowohl Daten als auch physische Dokumente) sicher gelöscht oder entsorgt werden, wenn sie nicht mehr benötigt werden
- Sicherstellung, dass Anwendungen Mandantenfähigkeit bieten oder dedizierte Systeme zur Verarbeitung von Daten für verschiedene Zwecke verwenden

4. **Trennung der Verarbeitung für verschiedene Zwecke**
   - Verwendung separater Entwicklungs-, Test-/Qualitätssicherungs- und Produktionsumgebungen
5. **Pseudonymisierung**
   - Sicherstellung, dass personenbezogene Daten aus Datensätzen entfernt (anonymisiert) werden, bevor diese für einen anderen Zweck verwendet werden, als für den sie ursprünglich erhoben wurden
6. **Verschlüsselung**
   - Verwendung von Verschlüsselung gemäß dem Stand der Technik (state-of-the-art) zur Sicherung von Daten im Ruhezustand (Data at Rest)

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

1. **Eingabekontrolle**
   - Aufzeichnung von Benutzeranmeldungen und fehlgeschlagenen Anmeldeversuchen
   - Protokollierung von Benutzerverwaltungsaktionen
   - Festlegung von Fristen für die Speicherung und Löschung von Protokolldaten
   - Sicherstellung der Eingabevalidierung
2. **Übertragungskontrolle**

- Koordinierung von Schnittstellenvereinbarungen
- Verwendung von Transport Layer Security (Authentifizierung und Verschlüsselung) für die Datenübertragung auf dem Stand der Technik (state-of the-art)
- Entkopplung des direkten externen Zugriffs auf die Anwendung
- Protokollierung der eingehenden und ausgehenden Datenkommunikation
- Sicherstellung von Ecoding für das entsprechende Zielsystem der Ausgabedaten

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. **Verfügbarkeitskontrolle**
   - Implementierung von Malware-Schutz (einschließlich EDR auf Clients und Servern)
   - Regelmäßiges Einholen/Anfordern von Informationen über Software-Schwachstellen
   - Behebung von Schwachstellen gemäß definierten Behebungszeiten, basierend auf der Kritikalität
   - Regelmäßige Identifizierung und Behebung von Schwächen
   - Implementierung von Backups gemäß einem Backup-Konzept
   - Sicherstellung, dass Backup-Wiederherstellungstests regelmäßig durchgeführt werden
   - Durchführung regelmäßiger Sicherheitsüberprüfungen auf Schwachstellen und Schwächen während der Entwicklung (statische und dynamische Sicherheitsanalyse)
   - Durchführung regelmäßiger Sicherheitsanalysen auf Schwachstellen und Verwundbarkeiten für größere Releases oder größere Feature-Änderungen (Penetrationstests)
   - Behebung identifizierter Schwachstellen und Verwundbarkeiten basierend auf ihrer Kritikalität
   - Bereithalten eines Cold-Standby-Systems
   - Sicherstellung angemessener physischer Maßnahmen zur Geschäftskontinuität für Rechenzentren und andere relevante IT-Infrastruktur (einschließlich redundanter Stromversorgung, Netzwerkverbindungen, Wasserschutz, Feuerlöschanlage)
   - Betrieb einer zentralen Organisation für das Schwachstellenmanagement für alle betroffenen Systeme

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (Art. 32 Abs. 1 lit. d DSGVO)

1. **Datenschutz-Management**
   - Bestätigung des Schutzbedarfs (Informationssicherheitsklassifizierung für die beteiligten Informationswerte)
   - Regelmäßige Überprüfung der Einhaltung der Serviceanforderungen
   - Berücksichtigung von Sicherheitsvorgaben bei der Entwicklung der Anwendung (Security by Design)
   - Berücksichtigung von Datenschutzanforderungen bei der Entwicklung der Anwendung (Privacy by Design)
   - Sicherstellung der Einhaltung von Compliance-Anforderungen und Regeln bei der Verwendung von Open-Source-Software
   - Planung und Dokumentation des Softwarelebenszyklus der Anwendung
   - Sensibilisierung der Anwendungsadministratoren für IT-Sicherheit
   - Betrieb eines Informationssicherheits-Managementsystems (ISMS) mit dedizierten Informationssicherheitsrollen, die für die Sicherstellung der Implementierung angemessener Informationssicherheitsmaßnahmen, die regelmäßige Bewertung ihrer Wirksamkeit und die Anpassung der Maßnahmen bei Bedarf verantwortlich sind
   - Betrieb eines Datenschutz-Managementsystems (DPMS) mit dedizierten Datenschutzrollen, die für die Sicherstellung der Dokumentation von Verarbeitungstätigkeiten, die Implementierung angemessener Datenschutzmaßnahmen, die regelmäßige Bewertung ihrer Wirksamkeit und die Anpassung der Maßnahmen bei Bedarf verantwortlich sind
2. **Incident-Response-Management**
   - Definition von Informationssicherheitsereignissen in Bezug auf Benutzeraktivitäten
   - Verwendung synchronisierter Zeitstempel bei der Protokollierung von Benutzeraktivitäten
   - Regelmäßige Analyse von Protokolldaten, um zu überprüfen, ob Informationssicherheitsereignisse oder -vorfälle aufgetreten sind
   - Betrieb einer 24/7-Incident-Response-Organisation, die sicherstellt, dass Informationssicherheitsereignisse zeitnah analysiert und darauf reagiert wird

- Aufrechterhaltung von Reaktionsplänen für relevante Informationssicherheitsvorfälle

3. **Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**
    - Sicherstellung, dass bei der Erhebung und Nutzung personenbezogener Daten nur die personenbezogenen Daten, die für einen bestimmten Zweck erforderlich sind, als obligatorisch gekennzeichnet werden
4. **Auftragskontrolle**
    - Sicherstellung, dass Unterauftragnehmer sorgfältig ausgewählt werden, Auftragsverarbeitungsverträge mit ihnen abgeschlossen werden und die technischen und organisatorischen Maßnahmen auch an die Unterauftragsverarbeitung weitergegeben werden
    - Sicherstellung, dass alle im Rahmen der Auftragsverarbeitung verwendeten personenbezogenen Daten am Ende des Servicevertrags gelöscht werden, es sei denn, es besteht eine gesetzliche Verpflichtung, sie länger aufzubewahren
    - Sicherstellung regelmäßiger Informationssicherheitsschulungen, einschließlich akzeptabler Nutzung beim Umgang mit Informationen, für alle Mitarbeiter, die Zugriff auf Anwendungsdaten haben
    - Sicherstellung, dass alle Mitarbeiter, die Zugriff auf personenbezogene Daten haben, zur Vertraulichkeit verpflichtet haben wurden