Anlage 2:
Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, vorläufig zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem Auftraggeber bei wesentlichen Änderungen und im Übrigen jährlich zur Durchführung der Auftragskontrolle vorzulegen.

Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen.

1. Pseudonymisierung
Wie wird die Pseudonymisierung der Daten gewährleistet?

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

- Personenbezogene Daten werden durch Zufallscodes ersetzt (bei statistischen Auswertungen)

2. Verschlüsselung
Wie wird die Verschlüsselung gewährleistet?

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

- Data Hashing
- Transportverschlüsselung (SSL/TLS)
- Nutzung von VPN
- Verschlüsselung von Datenträgern/Notebooks

3. Fähigkeit der Vertraulichkeit
Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet?

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Sicherheitsmaßnahmen RZ:

- Berechtigungsausweise (RFID)
- Zutritt nur für befugte Personen (Betriebsangehörige)
- Klingelanlage mit Kamera
- Anwesenheitsaufzeichnungen
- Besucherausweise

- Die Sicherung durch Alarmanlagen
- Definierte Sicherheitsbereiche
- RFID gesicherter Lieferanteneingang
- Türen sind gesichert durch elektrische Türschließer und Ausweisleser
- Sicherheitstüren und -fenster
- Videoüberwachung

Büro:

- Spezielle Schutzvorkehrungen für den Serverraum am Standort
    - Videoüberwachung
    - Zutrittsbeschränkungen
- VPN
- FTP/SSL/TLS
- Sorgfältige Auswahl von Dienstleistern
- Zutrittskontrolle (RFID)
- Verpflichtung der Mitarbeiter auf Vertraulichkeit
- Regelmäßige Schulungs- und Sensibilisierungsmaßnahmen
- Unternehmensrichtlinien
    - Passwort-Rl.
    - Clean Desk & Clear Screen
    - Verfahrensanweisungen
- Besondere Sicherungsmaßnahmen beim mobilen Arbeiten
- Vergabe von Berechtigung nach dem Need-to-Know-Prinzip
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen bei Eigenentwicklungen Privacy by Design & Default)

4. Fähigkeit der Integrität
Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet?

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern.

- Funktionelle Verantwortlichkeiten / Rollenkonzept
- Protokollierung von Zugriffen und Zugriffsversuchen
- 4-Augenprinzip bei Arbeiten an der IT-Infrastruktur
- Named User

5. Fähigkeit der Verfügbarkeit
Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet?

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- USV
- Viren- und Spamschutz
- Firewall

- CO_2-Löscher im Serverraum
- Temperatur- und Feuchtigkeitsfühler im Serverraum
- Netzwerksegmentierung
- Sorgfältige Auswahl von Dienstleistern
- Monitoring und Alerting
- Patchmanagement
- Spiegeln von Festplatten
- Klimaanlagen
- Brand- und Löschwasserschutz
- 4-Augenprinzip

6. Fähigkeit der Belastbarkeit
Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet?

Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

- Kapazitätsmanagement

7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs
Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?

- hochverfügbare technische Clusterumgebung
- Backup-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Vertretungsregelungen
- Wiederanlaufplan
- Regelmäßige BCM-Tests

8. Verfahren zur regelmäßigen Überprüfung
Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

- Datenschutzmanagement
- Auftrags- oder Vertragskontrolle
- Regelmäßige BCM-Tests
- Auditierung durch externen DSB

9. Unrechtmäßiger Zugang zu personenbezogenen Daten
Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

- Individueller Log-In und Kennwortverfahren
- Zusätzlicher Log-In für bestimmte Anwendungen
- Automatische Sperrung der Clients (Zeitablauf)
- Verwaltung und Review von Berechtigungen
- Monitoring
- Meldeverfahren

10. Verarbeitung personenbezogener Daten nur nach Anweisung
Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

- Mitarbeiter sind auf Verhaltensregeln verpflichtet
- Definierte Weisungsempfänger
- Implementierung unternehmensinterner Datenschutz-Richtlinien
- Verpflichtung der Mitarbeiter auf Vertraulichkeit
- Schulungen aller zugriffsberechtigten Mitarbeiter
- Rollenkonzept
- Kontrolle der Arbeitsergebnisse
- Dokumentation von Verantwortlichkeiten
- Verfahrensanweisungen