

Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers gemäß Art. 32 DSGVO

1. Vertraulichkeit

1. Zutrittskontrolle

- a. Elektronisches Zutrittskontrollsystem
 - i. Persönlicher Transponder
 - ii. Einteilung in Zonen (zum Beispiel je Gebäude, Bürotrakt)
 - iii. Onboarding-Prozess
 - iv. Elektrischer Türöffner an der Eingangstür und selbstschließende Außentüren
 - v. Im Rechenzentrum zusätzlich:
 1. Vereinzelungsschleuse
 2. Alarm bei nicht geschlossenen Türen
- b. Spezifische Zutrittsregelungen für Personengruppen
 - i. Anmeldung von Besuchern am Empfang
 - ii. Begleitung von Besuchern durch interne Mitarbeiter
 - iii. Im Rechenzentrum zusätzlich:
 1. Zutritt nur nach vorheriger namentlicher Anmeldung
 2. Verschlussene Serverräume mit Zutrittsberechtigung nur für autorisiertes Personal
- c. Überwachungs- und Alarmsysteme
 - i. Verwendung einer Alarmanlage und Alarmschleusen auf den Wachschatz
 - ii. Bei Alarm erfolgt Überwachung durch Wachschutz vor Ort
 - iii. Im Rechenzentrum zusätzlich:
 1. Videoüberwachung der Anlage durch dessen Betreiber

2. Zugangskontrolle

- a. Sichere Zugangsverbindungen und Technologien zur Authentifizierung sind implementiert, um den Zugang zu SysEleven Produktivsystemen und internen Support-Tools zu reglementieren.
 - i. Zugang zu internen Systemen wird durch Firewall- beziehungsweise VPN-Systeme beschränkt.
 - ii. Verschlüsselungstechniken werden eingesetzt, um Benutzerauthentifizierungen und Administrationsessions über das Internet abzusichern.
 - iii. Der Datenfernzugriff auf Produktionsmaschinen benötigt eine Verbindung zum Firmennetzwerk, die durch VPN-Systeme gesichert wird.
- b. Es besteht ein formaler Prozess, um den Zugang zu Ressourcen zu erlauben oder zu verweigern. Verschiedene Zugangsschutzmechanismen helfen dabei, sichere und flexible Zugriffe bereitzustellen.
- c. Die Erteilung oder Änderung von Zugangsrechten erfolgt auf Grundlage eines Berechtigungskonzepts.

3. Zugriffskontrolle

- a. Zugriff durch personalisierte Accounts auf Basis eines Berechtigungskonzepts
- b. Zugriffe werden protokolliert
- c. Arbeitsendgeräte verwenden eine Festplattenverschlüsselung
- d. Arbeitsendgeräte verwenden passwortgeschützte Accounts
- e. Arbeitsendgeräte unterliegen einem zentralen Monitoring

4. Trennungskontrolle

- a. Die Verarbeitung erfolgt auf Serversystemen, die durch logische und physische Zugriffskontrollen im Netzwerk getrennt sind (vgl. Abschnitte zur Zutritts-, Zugangs- und Zugriffskontrolle).

- b. Kundensysteme werden grundsätzlich projektspezifisch angelegt, soweit dies nicht individuell für ein Projekt anders geregelt ist.

- c. Trennung von Test- und Produktivsystemen

5. Pseudonymisierung

- a. Die Umsetzung der Pseudonymisierung von personenbezogenen Daten wird in Absprache mit dem Kunden für das jeweilige Projekt festgelegt.

2. Integrität

1. Weitergabekontrolle

- a. Der Zugriff auf die Systeme unterliegt der Zugriffskontrolle.
- b. Der Umgang mit Datenträgern ist formalisiert und in verbindlichen Anweisungen geregelt:
 - i. Verschlüsselung von Festplatten der Arbeitsrechner
 - ii. Verschlüsselung externer Datenträger
 - iii. Sicherstellung der ordnungsgemäßen Vernichtung physischer Datenträger durch zertifizierte Entsorgungsunternehmen bzw. Aktenvernichter
- c. Schutz der Netzwerke gegen Kompromittierung der Übertragung durch Firewalls und VPN
- d. Verschlüsselung von E-Mails mit sensiblen Informationen (optimale Leistung)

2. Eingabekontrolle

- a. Zur Eingabekontrolle werden System- und Anwendungslogs gespeichert und administrative Tätigkeiten aufgezeichnet (Protokollierung)

3. Verfügbarkeit

1. Verfügbarkeitskontrolle

- a. Unterbrechungsfreie Stromversorgung
- b. Einteilung der Betriebsflächen des Rechenzentrums in Brandabschnitte
- c. Einsatz von:
 - i. Brandfrüherkennung
 - ii. Brandmeldelanlage
 - iii. Brandlöschsystem und Feuerlöscher
- d. Optionale Leistungen:
 - i. Automatisiertes Monitoring
 - ii. Redundante Auslegung der Datenverarbeitungssysteme durch Spiegelung
 - iii. Regelmäßige Notfallübungen
 - iv. Virenschutz auf den Servern und Clients
 - v. Regelmäßige Prüfung der Server auf Schwachstellen (Security-Scans)

2. Rasche Wiederherstellbarkeit

- a. Versioniertes Konfigurationsmanagement für interne Systeme
- b. Optionale Leistungen:
 - i. Datensicherung gemäß Datensicherungskonzept
 - ii. Laufende Erstellung von Backups der Serverinhalte
 - iii. Regelmäßiger Test der Datenwiederherstellung

3. Belastbarkeit

- a. Die Umsetzung der Belastbarkeit der bereitgestellten Systeme wird in Absprache mit dem Kunden für das jeweilige Projekt festgelegt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Datenschutz-Management

- a. Bestellung eines Datenschutzbeauftragten
- b. Schriftliche Verpflichtung aller Mitarbeiter auf das Datengeheimnis
- c. Regelmäßige Datenschutzbildungen
- d. Einsatz verschließbarer Behälter zur Aufbewahrung von Datenträgern

2. Vorfall-Management

- a. Einsatz eines Ticketsystems zur Nachverfolgung von Vorfällen

3. Datenschutzfreundliche Voreinstellungen

- a. Die Umsetzung der datenschutzfreundlichen Voreinstellungen werden in Absprache mit dem Kunden für das jeweilige Projekt festgelegt.

4. Auftragskontrolle

- a. Vertragliche Regelungen zur Auftragsverarbeitung mit Unterauftragnehmern
- b. Risikoorientierte Überprüfung von Zertifizierungen von Unterauftragnehmern
- c. Risikoorientierte Durchführung von Kontrollen bei Unterauftragnehmern

5. Durchführung interner Kontrollmaßnahmen

- a. Regelmäßige Durchführung interner Kontrollmaßnahmen zur Sicherstellung und Überprüfung der Wirksamkeit ergriffener Maßnahmen durch den Auftragnehmer

Muster