Technisch Organisatorische Maßnahmen Version 39
Datum: 15. Jun 2023
Verfasser: Andreas Koch

## Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

*Zutrittskontrolle*

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

**Technische Maßnahmen der Zutrittskontrolle:**

- ☑ Gebäudesicherung (Gebäude ist nachts alarmgesichert)
- ☑ Chipkarten / Transpondersysteme
- ☑ Sicherheitsschlösser
- ☑ Türen mit Knauf Außenseite
- ☑ Videoüberwachung der Eingänge
- ☑ Alarmanlage (für OUTERMEDIA-Büroräume)
- ☑ Sicherheitsdienst (für OUTERMEDIA-Büroräume) **Organisatorische**

**Maßnahmen der Zutrittskontrolle:**

- ☑ Sicherheitsdienst (für OUTERMEDIA-Büroräume)
- ☑ Schlüsselregelung / Liste
- ☑ Besucher in Begleitung durch Mitarbeiter
- ☑ Sorgfalt bei Auswahl des Wachpersonals
- ☑ Sorgfalt bei Auswahl Reinigungsdienste

*Zugangskontrolle*

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen ergriffen werden, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

**Technische Maßnahmen der Zugangskontrolle**

- ☑ Login mit Benutzername + Passwort
- ☑ Anti-Viren-Software Server
- ☑ Firewall
- ☑ Intrusion Detection Systeme
- ☑ Einsatz VPN bei Remote-Zugriffen
- ☑ Verschlüsselung von Datenträgern
- ☑ BIOS Schutz (separates Passwort) ☑ Verschlüsselung von Notebooks / Tablet

☑ zertifikatsbasierte Zugriffsberechtigung ( Serverzugang via SSH nur mit Zertifikaten)

*Organisatorische Maßnahmen der Zugangskontrolle*

☑ Richtlinie „Sicheres Passwort“

☐ Richtlinie „Löschen / Vernichten“

☐ Richtlinie „Clean desk“

☑ Richtlinie Datenschutz und / oder Sicherheit

*Zugriffskontrolle*

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen.

**Technische Maßnahmen der Zugriffskontrolle:**

☑ Aktenschredder

☑ Externer Aktenvernichter (DIN 32757)

☑ Physische Löschung von Datenträgern

**Organisatorische Maßnahmen der Zugriffskontrolle:**

☑ Minimale Anzahl an Administratoren

☑ Datenschutztresor

☑ Verwaltung Benutzerrechte durch Administratoren

*Trennungskontrolle*

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

**Technische Maßnahmen der Zugriffskontrolle:**

☑ Trennung von Produktiv- und Testumgebung

☑ Physikalische Trennung (Systeme / Datenbanken / Datenträger) ☑ Mandantenfähigkeit relevanter Anwendungen

**Organisatorische Maßnahmen der Zugriffskontrolle:**

☑ Steuerung über Berechtigungskonzept

☑ Festlegung von Datenbankrechten

☑ Datensätze sind mit Zweckattributen versehen

## Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

☑ Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)

- ☑ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

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

*Verfügbarkeitskontrolle*

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

**Technische Maßnahmen der Verfügbarkeitskontrolle:**

- ☑ Feuer- und Rauchmeldeanlagen
- ☑ Serverraumüberwachung Temperatur und Feuchtigkeit
- ☑ Serverraum klimatisiert
- ☑ USV
- ☑ Schutzsteckdosenleisten Serverraum
- ☑ RAID System / Festplattenspiegelung

**Organisatorische Maßnahmen der Verfügbarkeitskontrolle:**

- ☑ Backup & Recovery-Konzept
- ☑ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ☑ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- ☑ Getrennte Partitionen für Betriebssysteme und Daten

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

*Datenschutz-Management*

- ☐ Software-Lösungen für Datenschutz-Management im Einsatz
- ☑ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- ☑ Regelmäßige Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen
- ☑ Externer Datenschutzbeauftragter
- ☑ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- ☑ Regelmäßige Sensibilisierung der Mitarbeiter
- ☑ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

*Incident Response Management*

**Technische Maßnahmen des Incident Response Managements:**

- ☑ Einsatz von Firewall und regelmäßige Aktualisierung
- ☑ Intrusion Detection System (IDS)

**Organisatorische Maßnahmen des Incident Response Managements:**

- ☑ Einbindung von DSB in Sicherheitsvorfälle und Datenpannen

*Auftragskontrolle (Outsourcing an Dritte)*

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

- ☑ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- ☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
- ☑ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
- ☑ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- ☑ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht