

Technische und organisatorische Maßnahmen (TOM) nach Art. 28 EU DSGVO

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

Im Folgenden werden die technischen und organisatorischen Maßnahmen geregelt, die bei der durch den Auftragnehmer erbrachten Dienstleistung gemäß Anlage zu Art. 28 EU DSGVO umgesetzt werden.

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

1.1. 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. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. 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

- Schlüsselregelung/-liste

Organisatorische Maßnahmen

- Empfang/Rezeption/Pförtner
- Manuelles Schließsystem
- Besucher in Begleitung durch Mitarbeiter
- Sorgfalt bei Auswahl des Reinigungsdienst

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können

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 notwendig sein, 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

- Login mit Benutzername + Passwort
(Sämtliche DV-Systeme sind mit einem Benutzer/Kennwort geschützt. Die erstellten Kennwörter haben eine Mindestlänge von 12 Zeichen, enthalten Groß- und Kleinbuchstaben und Zahl(en). Der Auftragnehmer verwendet für jedes DV-System und jeden Dienst innerhalb eines DV-Systems eigene Benutzer/Kennwörter.)

Organisatorische Maßnahmen

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Anti-Viren-Software Server
- Zentrale Passwortvergabe
- Anti-Virus-Software Clients
- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen/Vernichten“
- Firewall
- Allg. Richtlinie Datenschutz und/oder Sicherheit in Zusammenarbeit mit der Landesanstalt für Medien NRW
- Einsatz VPN bei Remote-Zugriffen
- Teilweise Sperre externer Schnittstellen (USB)
- Automatische Desktopsperre

1.3. 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. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen

- Aktenschredder
- Physische Löschung und „Zerstörung“ von Datenträgern

Organisatorische Maßnahmen

- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren

1.4. 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

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

Organisatorische Maßnahmen

- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten

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

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen

- Einsatz von VPN
- Bereitstellungen über verschlüsselte Verbindungen wie https

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie

lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Organisatorische Maßnahmen

- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Löschungen
- STUDIO 47 ist nicht in die Datenverwaltung und -pflege involviert. Sollte dies nötig werden, so ist STUDIO 47 mit einem spezifischen Benutzer und spezifischen Rechten auszustatten.

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

3.1. Verfügbarkeitskontrolle

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

Technische Maßnahmen

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- Serverraum klimatisiert
- USV
- Schutzsteckdosenleisten Serverraum
- RAID System / Festplattenspiegelung

Organisatorische Maßnahmen

- Backup & Recovery-Konzept
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten

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

4.1. Datenschutz-Management

Technische Maßnahmen

Software-Lösungen für Datenschutz-Management im Einsatz

Organisatorische Maßnahmen

Mitarbeiter auf Vertraulichkeit/Datengeheimnis verpflichtet

Regelmäßige Sensibilisierung der Mitarbeiter

Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden