Technische und organisatorische Maßnahmen (ToMs)

Stand: 2021-07-09

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

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.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

Technische Maßnahmen

- Manuelles Schließsystem
- Sicherheitsschlösser
- Schließsystem mit Codesperre
- Türen mit Knauf Außenseite

Organisatorische Maßnahmen

- Besucher in Begleitung durch Mitarbeiter

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).

Es existieren folgende Maßnahmen zur Zugangskontrolle:

Technische Maßnahmen

- Login mit Benutzername + Passwort
- Anti-Virus-Software Clients
- Anti-Virus-Software mobile Geräte
- Firewall
- Intrusion Detection Systeme
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablet

Organisatorische Maßnahmen

- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen / Vernichten“
- Richtlinie „Clean desk“
- Allg. Richtlinie Datenschutz und Sicherheit
- Mobile Device Policy
- Anleitung „Manuelle Desktopsperre“

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.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

Technische Maßnahmen

- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen

- Einsatz Berechtigungskonzepte
- 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.

Es existieren folgende Maßnahmen zur Trennungskontrolle:

Technische Maßnahmen

- Trennung von Produktiv, Test- und Entwicklungsumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen

Organisatorische Maßnahmen

- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten

Pseudonymisierung (Art. 32 Abs. 1 lit. a) DS-GVO; Art. 25 Abs. 1 DS-GVO)

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 entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Es existieren folgende Maßnahmen zur Pseudonymisierung:

Technische Maßnahmen

- Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (mögl. verschlüsselt)

Organisatorische Maßnahmen

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

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

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.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

Technische Maßnahmen

- Einsatz von VPN
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Nutzung von Signaturverfahren

Organisatorische Maßnahmen

- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Weitergabe in anonymisierter oder pseudonymisierter Form

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.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

Technische Maßnahmen

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatisierte Kontrolle der Protokolle

Organisatorische Maßnahmen

- Klare Zuständigkeiten für Löschung

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. c) DS-GVO)

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.

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

Technische Maßnahmen

- RAID System / Festplattenspiegelung
- Daten- und Service Cluster über mehrere Verfügbarkeitszonen verteilt
- Automatisierter Systemtest durch End-to-End Tests

Organisatorische Maßnahmen

- Backup & Recovery-Konzept (ausformuliert)
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

Rasche Wiederherstellung (Art. 32 Abs. 1 lit. c) DSGVO)

Maßnahmen, die gewährleisten, dass die Cloud-Infrastruktur und das Backend das höchste mögliche Maß an Verfügbarkeit hat.

Es existieren folgende Maßnahmen zur raschen Wiederherstellung:

Technische Maßnahmen

- Hohe Erreichbarkeit

Organisatorische Maßnahmen

- Regelmäßige Schulung der Mitarbeiter auf Ausfallsszenarien und Recovery-Maßnahmen
- Ausfallsszenarien und Recovery-Maßnahmen
- Notfall Wiederherstellungsplan

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

Technische Maßnahmen

- Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)
- Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

Organisatorische Maßnahmen

- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnisverpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Privacy by design / Privacy by default

Technische Maßnahmen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen
- Datenschutz-Präferenz mit Cookies- und Datenschutz-Einstellungen

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.

Organisatorische Maßnahmen

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.