

Technische und organisatorische Massnahmen (TOM)

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.

Stand: 11. Dezember 2023

Inhaltsverzeichnis

1	Vertraulichkeit	3
1.1	Zutrittskontrolle.....	3
1.2	Zugangskontrolle.....	3
1.3	Zugriffskontrolle.....	3
1.4	Trennungskontrolle.....	4
1.5	Pseudonymisierung.....	4
2	Integrität.....	4
2.1	Weitergabekontrolle	4
2.2	Eingangskontrolle.....	5
3	Verfügbarkeit und Belastbarkeit	5
3.1	Verfügbarkeitskontrolle.....	5
4	Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung	6
4.1	Datenschutz-Massnahmen.....	6
4.2	Incident-Response-Management	6
4.3	Datenschutzfreundliche Voreinstellungen	6
4.4	Auftragskontrolle (Outsourcing an Dritte)	7

1 Vertraulichkeit

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	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Chipkarten / Transpondersysteme	<input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner
<input checked="" type="checkbox"/> Manuelles Schliesssystem	<input type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input type="checkbox"/> Mitarbeiter- / Besucherausweise
<input checked="" type="checkbox"/> Absicherung der Gebäudeschächte	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Videoüberwachung der Eingänge	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste

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 Bootpassword, Benutzererkennung 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	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Login mit Benutzername + Passwort	<input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen
<input checked="" type="checkbox"/> Login mit biometrischen Daten	<input checked="" type="checkbox"/> Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/> Anti-Viren-Software Server	<input checked="" type="checkbox"/> Zentrale Passwortvergabe
<input checked="" type="checkbox"/> Anti-Virus-Software Clients	<input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“
<input checked="" type="checkbox"/> Anti-Virus-Software mobile Geräte	<input checked="" type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Richtlinie „Clean desk“
<input checked="" type="checkbox"/> Mobile Device Management	<input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input checked="" type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	<input checked="" type="checkbox"/> Mobile Device Policy
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	<input checked="" type="checkbox"/> Anleitung „Manuelle Desktopsperre“
<input checked="" type="checkbox"/> BIOS Schutz (separates Passwort)	
<input checked="" type="checkbox"/> Automatische Desktopsperre	
<input checked="" type="checkbox"/> Verschlüsselung von Notebooks / Tablet	

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	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Aktenschredder (mind. Stufe 3, cross cut)	<input checked="" type="checkbox"/> Einsatz Berechtigungskonzepte
<input checked="" type="checkbox"/> Physische Löschung von Datenträgern	<input checked="" type="checkbox"/> Minimale Anzahl an Administratoren
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Datenschutztresor
	<input checked="" type="checkbox"/> 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	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Trennung von Produktiv- und Test- umgebung	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept
<input checked="" type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger)	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten
<input checked="" type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	<input checked="" type="checkbox"/> Datensätze sind mit Zweckattributen versehen

1.5 Pseudonymisierung

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;

Technische Massnahmen	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	<input checked="" type="checkbox"/> Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschrfrist möglichst zu anonymisieren / pseudonymisieren

2 Integrität

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	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Passwort Weitergabe nur verschlüsselt	<input checked="" type="checkbox"/> Dokumentation der Datenempfänger sowie der Dauer der geplanten Über- lassung bzw. der Löschrfristen
<input checked="" type="checkbox"/> Einsatz von VPN	<input checked="" type="checkbox"/> Übersicht regelmässiger Abruf- und Übermittlungsvorgängen
<input checked="" type="checkbox"/> Protokollierung der Zugriffe und Abrufe	<input checked="" type="checkbox"/> Weitergabe in anonymisierter oder pseudonymisierter Form
<input checked="" type="checkbox"/> Sichere Transportbehälter	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
<input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

2.2 Eingangskontrolle

Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingangskontrolle 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.

Technische Massnahmen	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input checked="" type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	<input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	<input checked="" type="checkbox"/> Klare Zuständigkeiten für Löschungen

3 Verfügbarkeit und Belastbarkeit

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, Raidssysteme, Plattenspiegelungen etc.

Technische Massnahmen	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Feuerlöscher Serverraum	<input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input checked="" type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input checked="" type="checkbox"/> USV	<input checked="" type="checkbox"/> Regelmässige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums
<input checked="" type="checkbox"/> RAID System / Festplattenspiegelung	<input checked="" type="checkbox"/> Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input checked="" type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	<input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundsatz 100-4)
	<input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten

4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Massnahmen

Technische Massnahmen	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Software-Lösungen für Datenschutz-Management im Einsatz	<input checked="" type="checkbox"/> Interner / externer Datenschutzbeauftragter (siehe Datenschutz)
<input checked="" type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
<input checked="" type="checkbox"/> Anderweitiges dokumentiertes Sicherheitskonzept	<input checked="" type="checkbox"/> Regelmässige Sensibilisierung der Mitarbeiter mindestens jährlich
<input checked="" type="checkbox"/> Eine Überprüfung der Wirksamkeit der technischen Schutzmassnahmen wird mind. jährlich durchgeführt	<input checked="" type="checkbox"/> Interner / externer Informationssicherheitsbeauftragter (siehe Datenschutz)
	<input checked="" type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach
	<input checked="" type="checkbox"/> Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Massnahmen	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Einsatz von Firewall und regelmässige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmässige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmässige Aktualisierung	<input type="checkbox"/> Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
	<input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	<input checked="" type="checkbox"/> Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technische Massnahmen	Organisatorische Massnahmen
<input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
<input checked="" type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Massnahmen	

4.4 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.

Technische Massnahmen	Organisatorische Massnahmen
	<input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmassnahmen und deren Dokumentation
	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln