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

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
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Chipkarten / Transpondersysteme	☒ Empfang / Rezeption / Pförtner
☒ Manuelles Schliesssystem	☐ Besucherbuch / Protokoll der Besucher
☒ Sicherheitsschlösser	☐ Mitarbeiter- / Besucherausweise
☒ Absicherung der Gebäudeschächte	☒ Besucher in Begleitung durch Mitarbeiter
☒ Videoüberwachung der Eingänge	☒ Sorgfalt bei Auswahl des Wachpersonals
	☒ 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 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	Organisatorische Massnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort“
☒ Anti-Virus-Software mobile Geräte	☒ Richtlinie „Löschen / Vernichten“
☒ Firewall	☒ Richtlinie „Clean desk“
☒ Mobile Device Management	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Einsatz VPN bei Remote-Zugriffen	☒ Mobile Device Policy
☒ Verschlüsselung von Datenträgern	☒ Anleitung „Manuelle Desktopsperre“
☒ BIOS Schutz (separates Passwort)	
☒ Automatische Desktopsperre	
☒ 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
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Physische Löschung von Datenträgern	☒ Minimale Anzahl an Administratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Datenschutztresor
	☒ 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
☒ Trennung von Produktiv- und Test- umgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ 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 technichen und organisatorischen Massnahmen unterliegen;

Technische Massnahmen	Organisatorische Massnahmen
☒ Im Falle der Pseudonymisierung: 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

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
☒ Passwort Weitergabe nur verschlüsselt	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Über- lassung bzw. der Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmässiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Sichere Transportbehälter	☒ Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
☒ 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. 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.

Technische Massnahmen	Organisatorische Massnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verar- beitungen übernommen wurden
	☒ 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, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

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

4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Massnahmen

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

4.2 ncident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Massnahmen	Organisatorische Massnahmen
☒ Einsatz von Firewall und regelmässige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmässige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmässige Aktualisierung	☐ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor-fällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technische Massnahmen	Organisatorische Massnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufrechts 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
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmass- nahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln