Technisch–organisatorische Maßnahmen (TOMs)

Es handelt sich hier um eine beispielhafte Aufzählung. Bitte prüfen Sie in Ihrem Unternehmen die durchzuführenden Maßnahmen und dokumentieren Sie diese ordentlich.

Mittels **Zutrittskontrollen** soll unbefugten Personen der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt werden.

Technische Maßnahmen: z.B. Alarmanlage, Automatisches Zugangskontrollsystem, Chipkartensystem, Lichtschranken, Bewegungsmelder, Türsicherung (Sicherheitsschlösser,elektrischer Türschließer, Ausweisleser,…)

Organisatorische Maßnahmen: z.B. Personenkontrolle beim Eingang, Besucherdokumentation und Gästeausweise, Zugang nur mit Schlüssel oder Mitarbeiterausweis, Videoüberwachung, …

Zugangskontrollen sollen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen: z.B. Authentifikation mit Benutzer und Passwort, Einsatz von Anti-Viren-Software, Firewalls und VPN Technologie, Sperren von externen Schnittstellen (zB USB Anschlüsse), Verschlüsselung von Datenträgern und Smartphones

Organisatorische Maßnahmen: z.B. Benutzerberechtigungen, Passwortvergabe, sorgfältige Auswahl von Reinigungs – und Sicherheitspersonal

Zugriffskontrollen sollen gewährleisten, dass nur die zur Benutzung Berechtigten auf die Daten zugreifen können und personenbezogene Daten nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen: Einsatz von Aktenvernichtern, Kontrollierte Vernichtung von Datenträgern, Löschung von Datenträgern vor deren Wiederverwendung, Protokollierung der Vernichtung von Daten, Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten, Verschlüsselung von Datenträgern und Smartphones

Organisatorische Maßnahmen: Anzahl der Administratoren gering halten, Erstellen eines Berechtigungskonzepts, sichere Aufbewahrung von Datenträgern, zusätzliche Sicherheitskopien außer Haus aufbewahren

Auch die Weitergabe von personenbezogenen Daten bedarf einer entsprechenden Kontrolle, sodass diese von Unbefugten weder gelesen, kopiert, verändert oder entfernt werden können. Weiters muss gewährleistet werden, dass die personenbezogenen Daten an die vorgesehenen Stellen übermittelt werden.

Technische Maßnahmen: Einrichtungen von VPN-Tunneln, E-Mail-Verschlüsselung
Organisatorische Maßnahmen: Dokumentation der Empfänger von Daten, Dokumentation der Löschung, Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Durch eine **Eingabekontrolle** soll überprüft und festgestellt werden, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt werden.

Technische Maßnahmen: Protokollierung der Eingabe, Änderung und Löschung von Daten
Organisatorische Maßnahmen: Nachvollziehbarkeit von Eingabe, Änderung und Löschung durch individuelle Benutzern, Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Durch eine **Auftragskontrolle** muss gewährleistet sein, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Organisatorische Maßnahmen: Auswahl des Auftragnehmers im Sinne der DS-GVO (EU oder Privacy Shield zertifiziert), auf Datenschutz im Auftragsverarbeitungsvertrag achten, Verpflichtung der Mitarbeiter des Auftragnehmer das Datengeheimnis zu wahren

Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden.

Technische Maßnahmen: Klimaanlage in Serverräumen, Feuer- und Rauchmeldeanlagen , Feuerlöschgeräte, Unterbrechungsfreie Stromversorgung (USV)

Organisatorische Maßnahmen: Versperrbare Serverräume, Erstellen eines Backup- & Recoverykonzepts, Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort, Testen von Datenwiederherstellung zumindest alle 6 Monate