MELTING MIND

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 24, 25, 32 DSGVO

MELTING MIND Fabian Schmidt
Albert-Lezius-Straße 92b
23562 Lübeck

Aktuelle Version vom 25.09.2023

Das vorliegende Dokument beschreibt die Anforderungen und die Umsetzung der Maßnahmen für einen sicheren und datenschutzkonformen Umgang mit personenbezogenen Daten, um ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten. Das o.g. Unternehmen erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. 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	Organisatorische Maßnahmen
Zutrittssperren mit Chipkarten / Transpondersystemen	Dokumentierte Schlüsselregelung / -ausgabe
Manuelle Schließsysteme	Empfang / Rezeption
Sicherheitsschlösser	Besucher in Begleitung durch Mitarbeiter
Verschlossene Serverräume mit separater Zutrittskontrolle	

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
Einsatz von VPN bei Remote-Zugriffen	Erstellung von Benutzerprofilen
Anti-Viren-Software Server	Zentrale Passwortvergabe
Anti-Virus- Software Clients	Richtlinie „Sicheres Passwort"
Firewall	Richtlinie „Löschen / Vernichten"
Intrusion Detection Systeme	Richtlinie „Clean Desk"
Mobile Device Management	Allg. Richtlinie Datenschutz und/ oder Sicherheit
Verschlüsselung von Datenträgern	Mobile Device Policy
Verschlüsselung Smartphones	Anleitung „Manuelle 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	Organisatorische Maßnahmen
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz rollenbasierter Berechtigungskonzepte
Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	Minimale Anzahl Administratoren
Physische Löschung von Datenträgern	Verwaltung Benutzerrechte durch Administratoren
Verschlüsselung mobiler Datenträger	Geschützte Aufbewahrung der Datenträger

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 Testumgebung	Steuerung über Berechtigungskonzept
Physikalische Trennung (Systeme / Datenbanken /Datenträger)	Festlegung von Datenbankrechten
Mandantenfähigkeit relevanter Anwendungen	Datensätze sind mit Zweckattributen versehen

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a. DSGVO; Art. 25 Abs. 1 DSGVO)

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
Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisierten / pseudonymisieren

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	Organisatorische Maßnahmen
S/MIME E-Mail-Verschlüsselung / Signierung	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
Einsatz von VPN	Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge
Protokollierung der Zugriffe und Abrufe	Weitergabe in anonymisierter oder pseudonymisierter Form
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	Persönliche Übergabe mit Protokoll

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.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden
Überwachung und Protokollierung der elektronischen Datenverarbeitung	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 Berechtigungskonzeptes
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	Klare Zuständigkeiten für Löschungen

2.3. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des AuTraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im AuTrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der AuTragnehmer 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 Sicherheitsmaßnahmen und deren Dokumentation
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Schriftliche Weisungen an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	Regelung zum Einsatz weiterer Subunternehmer
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	Dokumentation der Verarbeitungsprozesse

3. Verfügbarkeiten 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, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept
Feuerlöscher Serverraum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Klimatisierter Serverraum	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraum
Unterbrechungsfreie Stromversorgung (USV)	Existenz eines Notfallplan (z.B. BSI IT-Grundschutz 100-4)
Schutzsteckdosenleisten Serverraum	Getrennte Partitionen für Betriebssysteme und Daten
RAID System / Festplattenspiegelung	
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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

4.1. Datenschutz-Management

Maßnahmen zur Überwachung der Einhaltung der Bestimmungen zum Datenschutz in angemessener Weise. Dieses Verfahren muss u.a. die Dokumentation aller für den Auftraggeber durchgeführten Verarbeitungstätigkeiten vor Beginn der Auftragsverarbeitung, die Unterrichtung und Sensibilisierung von Mitarbeitern sowie ihre Verpflichtung auf das Datengeheimnis als auch die regelmäßige Überwachung und Auditierung der angewendeten Datenverarbeitungsverfahren, sicherstellen. Es besteht ein Prozess für eine schnelle und effektive Wahrnehmung von Betroffenenrechten und Meldung von Datenschutzverstößen. Dieser Prozess muss auch die Überwachung des Auftraggebers beinhalten.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Software-Lösung für Datenschutzmanagement	Benennung eines internen Datenschutzbeauftragten
Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (mind. jährlich)	Regelmäßige Sensibilisieren der Mitarbeiter (mind. jährlich)
Dokumentiertes Sicherheitskonzept	Mitarbeiter geschult auf Vertraulichkeit / Datengeheimnis verpflichtet
Regelmäßige Überprüfung des Stands der Technik	Regelmäßige Prüfung der Verfahren im Rahmen des QMS
	Regelmäßige Prüfung der Auftragsverarbeiter
	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
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch in Hinblick auf die Meldepflicht gegenüber Aufsichtsbehörden)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
Einsatz von Virenscanner und regelmäßige Aktualisierung	Einbindung von Datenschutzbeauftragten und internem Sicherheitsbeauftragten in Sicherheitsvorfälle und Datenpannen
Intrusion detection system (IDS)	Dokumentation von Sicherheitsvorfällen und Datenpannen im Ticketsystem
Intrusion prevention system (IPS)	Formaler Prozess und Verantwortlichkeiten zur Nachbereitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

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 Widerrufsrechts des Betroffenen durch technische Maßnahmen	