Mahr EDV
Störungsfrei arbeiten!

TOM - Technische und organisatorische Maßnahmen

Revision: 5
Freigabedatum: 23.04.2026 12:51
Nr.: D20427000
Prüfer: Alexander Pohl

Inhaltsverzeichnis

1. Zweck des Dokuments

Die Mahr EDV verarbeitet personenbezogene Daten. Um den Anforderungen der Datenschutz-Grundverordnung (DSGVO) gerecht zu werden, implementieren wir spezifische Sicherheitsvorkehrungen. Dieses Dokument dient der Dokumentation dieser Maßnahmen, die das Ziel verfolgen, Daten vor unbefugtem Zugriff, Verlust oder Missbrauch zu schützen. Es deckt sowohl technische Aspekte (z.B. IT-Sicherheit, Verschlüsselung) als auch organisatorische Verfahren (z.B. Schulungen, Zutrittsregelungen) ab. Dieses Dokument dient zudem als Nachweis der Einhaltung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

2. Geltungsbereich

Die TOMs gelten für alle Abteilungen und Mitarbeiter, die Zugriff auf personenbezogene Daten haben

3. Definition

-

4. Auftragskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Regelungen zur datenschutzgerechten Löschung und Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Schriftliche Weisungen an den Auftragnehmer
- Vertragsstrafen oder vergleichbare Sanktionsmechanismen bei Verstößen, soweit vereinbart
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit und Datenschutz
- Abschluss einer Auftragsverarbeitungsvereinbarung
- Schulung, Prüfung, Besichtigung im erforderlichen Umfang

5. Datenschutz-Management

Ziel: Gewährleistung des Daten- und Vertraulichkeitsschutzes durch regelmäßige Prüfung und Evaluierung

- Mahr EDV hat Datenschutzbeauftragten bestellt
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- Mitarbeiterschulungen
- Sicherheitskonzept
- Verpflichtungsvereinbarungen zum Datenschutz und Informationssicherheit
- Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen
- Durchführung von Datenschutz-Folgenabschätzung
- Interne Revisionen und Kontrollen
- Erfüllung der Informationspflichten gemäß DSVGO und BDSG
- Einrichtung und Beachtung von Löschsperren, soweit erforderlich

6. Eingabekontrolle

Ziel: Protokollierung auch zur nachträglichen Prüfung, ob, wer und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt hat.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Klare Verantwortung für Löschungen und Sperrungen
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzerkennungen
- Passwortschutz
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Benutzerauthentifizierung
- Zweifaktorauthentifizierung
- Monitoring
- Regelmäßige Sicherheitsprüfungen

7. Incident-Response-Management

Ziel: Gewährleistung einer strukturierten Reaktion auf Sicherheitsverletzungen

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
- Dokumentation von Sicherheitsvorfällen
- Schadsoftwareschutz
- Einbindung des DSB, soweit erforderlich
- Firewall
- Spamfilter
- Intrusion Prevention System
- Ticketsystem
- Regelmäßige Sicherheitsprüfungen

8. Privacy by Design

Ziel: Voreinstellung von Systemen zur Datensparsamkeit

- Es werden nur solche personenbezogenen Daten erhoben und verarbeitet, die für den jeweiligen Zweck erforderlich sind
- Datenschutzfreundliche Voreinstellungen in Systemen und Anwendungen
- Technische Maßnahmen zur einfachen Ausübung von Betroffenenrechten, insbesondere des Widerrufsrechts, soweit einschlägig

9. Pseudonymisierung

Ziel: Sicherstellung, dass Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können

- Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System, möglichst verschlüsselt
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren oder zu pseudonymisieren

10. Trennungskontrolle

Ziel: Sicherstellung, dass zu unterschiedlichen Zwecken erhobene Daten nur getrennt verarbeitet werden können.

- Physikalisch oder logisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten
- Erstellung und Umsetzung eines Berechtigungskonzepts
- Logische Mandantentrennung auf Anwendungsebene
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

11. Verfügbarkeitskontrolle

Ziel: Schutz der Daten vor zufälliger Zerstörung oder Verlust.

- USV und Notstrom
- Bewegungsmelder, Videoüberwachung, 24/7 Aufschaltung zum Sicherheitsdienst
- Klimaanlage und Temperatur- und Feuchtemonitoring in Serverräumen
- Backup- & Recoverykonzept sowie Havariepläne
- RAID Systeme und Komponentenredundanz, RZ-Redundanz
- Regelmäßiger Test und Protokollierung Datenwiederherstellung
- Schutzsteckdosen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Brandfrüherkennung, Feuerlöschsysteme

12. Weitergabekontrolle

Ziel: Schutz der Daten auf jeglichen Transportwegen vor dem Zugriff Dritter (einschließlich des Lesens, Kopierens, Änderns, Entfernens) und Sicherstellung der Nachvollziehbarkeit sämtlicher Datenweitergaben.

- Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- Einrichtung von verschlüsselten VPN-Tunneln
- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Elektronische Verschlüsselung
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verwendung sicherer Transportbehälter/-verpackungen
- Protokollierung der Nutzung

13. Zugangskontrolle

Ziel: Beschränkung der Nutzung von Datenverarbeitungsanlagen auf Befugte

- Benutzerrollen und Rechte geregelt und den jeweiligen Systemen und Anwendungen zugeordnet
- Authentifizierung mit Benutzername/Passwort
- Verschlüsselung von PCs ,Notebooks, Datenträgern, Smartphones
- Mobile-Device-Management
- Passwortkomplexitätsrichtlinien, Passwortänderungsrichtlinien und -überwachung bzw. automatische Zugangssperre
- Sorgfältige Auswahl von Wach und Reinigungspersonal sowie ggf. begleiteter Zugang
- Sicherheitsschlösser/Verriegelungen (physisch), Abschaltung von Schnittstellen (bspw. USB)

- VPN/Verschlüsselung/https
- Intrustion-Detection-Systeme, Firewalls, Virenschutz
- Schlüsselregelung
- Benutzerschulungen

14. Zugriffskontrolle

Ziel: Beschränkung des Zugriffs auch berechtigter Nutzer von Datenverarbeitungsanlagen auf die jeweils notwendigen Daten.

- Berechtigungsstufen und -konzepte
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Verschlüsselung von Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Beschränkung der Anzahl von Administratoren auf das erforderliche Maß
- Sichere Aufbewahrung von Datenträgern
- Vergabe und Verwaltung der Rechte durch autorisierte Administratoenr
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399/ISO 21964)

15. Zutrittskontrolle

Ziel: Beschränkung des Zutritts zu Datenverarbeitungsanlagen auf Befugte

- Alarmanlage
- Sorgfältige Auswahl von Wachpersonal/Reinigungsdiensten
- Automatisches Zugangskontrollsystem
- Absicherung von Gebäudeschächten
- Schließsystem mit Codesperre
- Videoüberwachung
- Lichtschranken / Bewegungsmelder
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Empfang und Besucherbegleitung

16. Authentizitätskontrolle

Ziel: Sicherstellung, dass nur eindeutig identifizierte und autorisierte Personen oder Systeme auf Datenverarbeitungssysteme zugreifen, Daten verarbeiten oder Verarbeitungsvorgänge auslösen können und dass diese Handlungen eindeutig einer verantwortlichen Stelle zugeordnet werden können.

- Eindeutige Vergabe von Benutzerkennungen
- Keine Verwendung von Sammel- oder Gemeinschaftskonten, soweit technisch vermeidbar
- Benutzerauthentifizierung durch individuelle Benutzername-/Passwort-Kombinationen
- Einsatz von Zweifaktorauthentifizierung, insbesondere bei administrativen Zugängen, Fernzugriffen und sonstigen besonders schutzbedürftigen Zugängen
- Dokumentierte Verfahren zur Einrichtung, Änderung, Sperrung und Löschung von Benutzerkonten
- Dokumentierte Vergabe und Entziehung von Berechtigungen
- Regelmäßige Überprüfung von Benutzerkonten und Berechtigungen
- Protokollierung von Anmeldungen, Zugriffsversuchen und administrativen Tätigkeiten
- Nachvollziehbare Zuordnung von Eingaben, Änderungen und Löschungen zu individuellen Benutzerkonten

- Besondere Absicherung von Administratoren- und privilegierten Konten
- Regelungen zum Umgang mit technischen Konten, Service-Accounts und Schnittstellenzugängen
- Authentifizierung von Systemen und Absicherung von System-zu-System-Kommunikation
- Schutz von Authentifizierungsdaten vor unbefugter Kenntnisnahme und Verwendung
- Einsatz von Zertifikaten, Signaturverfahren oder vergleichbaren technischen Verfahren, soweit erforderlich
- Regelmäßige Prüfung der Wirksamkeit der eingesetzten Authentifizierungsverfahren