Technische und organisatorische Maßnahmen (TOMs)

gem. Art. 32 DSGVO

der Luehrsen Heinrich GmbH

Stand: 22.10.2024

Präambel

Die Luehrsen Heinrich GmbH hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert. Der allgemeine Teil (Grundsätzliche Maßnahmen) beschreibt technische und organisatorische Maßnahmen, die unabhängig von den jeweiligen Dienstleistungen, Standorten und Kunden gelten. In den darauf folgenden Abschnitten sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1. Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Ein betriebliches Datenschutz-Management ist implementiert, dessen Einhaltung systematisch überwacht sowie mindestens einmal jährlich evaluiert wird.
- Es besteht ein Konzept, das eine unverzügliche und gesetzeskonforme Reaktion auf Datenschutzverletzungen (Prüfung, Dokumentation, Meldung) gewährleistet.
- Die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung) erfolgt innerhalb der gesetzlichen Fristen.
- Berechtigungen, Zugangskarten, Schlüssel und Codes werden nach Ausscheiden von Mitarbeitern oder Wechsel der Zuständigkeiten entzogen.
- Alle Mitarbeiter werden regelmäßig im Bereich Datenschutz und Datensicherheit geschult und auf Verschwiegenheit verpflichtet.
- Mitarbeiter erhalten personalisierte Accounts, wo möglich, um Verantwortlichkeiten klar zu trennen.
- Übergebene Passwörter und Zugänge werden sicher in einem Passwort-Manager (1Password) verwaltet.

2. Zutrittskontrolle

Maßnahmen, um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen zu verhindern:

- Einsatz von Alarmanlagen
- Chipkarten-/Transpondersysteme für den Zugang
- Videoüberwachung der Eingänge
- Sorgfältige Auswahl von Wachpersonal und Reinigungsdiensten
- Sicherstellung der Zutrittskontrolle durch manuelle Schließsysteme
- Permanente Überwachung von Eingängen und Schlüsselausgabe
- Zutrittsregelung für Besucher (z. B. durch Begleitung durch Mitarbeiter)

3. Zugangskontrolle / Zugriffskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden:

- Login mit Benutzername und Passwort
- Verwaltung von Benutzerberechtigungen und Benutzerprofilen
- Einsatz eines Passwort-Managers (1Password) für die sichere Verwaltung von Zugangsdaten
- Richtlinie für starke Passwörter
- Regelmäßige Updates von Virenscannern und Firewalls
- Automatische Desktopsperren und Verschlüsselung von Endgeräten wie Smartphones, Notebooks und Tablets
- Verschlüsselung des Datentransfers über https/TLS oder vergleichbare Schutzsysteme
- Netzwerk-Firewall zur zusätzlichen Absicherung
- Minimierung der Anzahl der Administratoren und klare Verantwortlichkeiten

4. Weitergabekontrolle

Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei der Übertragung oder Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können:

- Protokollierung der Zugriffe und Abrufe
- Daten werden nur an autorisierte Dritte weitergegeben
- Verschlüsselung von Datenträgern und Verbindungen (sftp, https)
- Pseudonymisierung von Daten, wo sinnvoll
- Dedizierte Weitergabeberechtigungen

5. Eingabekontrolle

Maßnahmen, um nachträglich festzustellen, ob und von wem personenbezogene Daten in das System eingegeben, verändert oder entfernt wurden:

- Protokollierung von Dateneingaben, -änderungen und -löschungen
- Übersicht über verwendete Programme zur Datenverarbeitung
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung durch individuelle Benutzernamen (keine Gruppenaccounts)
- Berechtigungssteuerung zur Eingabe und Bearbeitung von Daten basierend auf einem Berechtigungskonzept

6. Auftragskontrolle

Maßnahmen, um sicherzustellen, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Vorherige Prüfung der Sicherheitsmaßnahmen des Auftragnehmers
- Sorgfältige Auswahl von Auftragnehmern, insbesondere hinsichtlich Datenschutz und Datensicherheit
- Abschluss von Auftragsverarbeitungsverträgen (AVV)
- Schriftliche Weisungen an Auftragnehmer zur Datenverarbeitung
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Vereinbarung von Kontrollrechten und Regelungen zum Einsatz von Subunternehmern

7. Verfügbarkeitskontrolle / Integrität

Maßnahmen, um sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backup- und Recovery-Konzept mit 7-tägiger Aufbewahrung von Sicherungen
- Einsatz von RAID-Systemen zur Festplattenspiegelung
- Einsatz von Virenschutz, Anti-Spyware und Spamfiltern
- Differenzielle und Vollsicherung von Daten (cloudbasiert und auf NAS-Systemen)
- Notfallkonzept zur Wiederherstellung durch interne IT und externe Dienstleister

8. Gewährleistung des Zweckbindungs-/Trennungsgebotes

Maßnahmen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung von Systemen, Datenbanken und Datenträgern
- Steuerung der Verarbeitung durch ein Berechtigungskonzept