

Technische und organisatorische Maßnahmen (TOMs)

gem. Art. 32 DSGVO

Dr. Daria Podwika, iexplainia

Stand: 06.10.2026

Hinweis

Dieses Dokument enthält Informationen, welche Geschäftspartnern, Kunden sowie weiteren externen Stellen, die ein gesetzliches oder sonstig begründetes Einsichtsrecht haben, zur Verfügung gestellt werden. Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

Präambel

Der Verantwortliche 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 und Services, 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:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung systematisch überwacht sowie anlassbezogen und mindestens halbjährlich evaluiert wird.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und alle notwendigen Umsetzungsverfahren.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe und Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren.

- Die im Hinblick auf die Verarbeitung personenbezogener Daten erteilten Berechtigungen sowie ausgegebenen Schlüssel, Zugangskarten oder Codes jeglicher Art an externe Dienstleister, Freelancer oder sonstige Beauftragte, werden nach Beendigung des jeweiligen Vertragsverhältnisses bzw. bei Wegfall der Notwendigkeit des Zugriffs gemäß eines Berechtigungskonzeptes unverzüglich eingezogen bzw. entzogen.
- Alle Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (z.B. Reinigungs-, Wachpersonal, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Bei Dienstleistern, die nicht nebengeschäftlich tätig werden, wird der Schutz von personenbezogenen Daten und die Sicherung der Rechte und Pflichten von Auftraggebern/Auftragnehmern einer Auftragsverarbeitung gewährleistet. Dies gilt auch für vergleichbare Situationen mit einem Datentransfer in sogenannte Drittstaaten.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virens Scanner und Firewalls.

2. Zutrittskontrolle

Alle Maßnahmen, die dazu geeignet sind, den Zutritt für Unbefugte zu den Datenverarbeitungsanlagen zu verhindern.

Umgesetzte Maßnahmen:

- Manuelles Schließsystem
- Türen mit Knauf Außenseite
- Dienstliche Unterlagen und Geräte sind für Haushaltsangehörige und Gäste nicht zugänglich
- Der Arbeitsbereich ist separat oder abschließbar und von Dritten nicht einsehbar
- Beim Verlassen des Arbeitsplatzes wird der Bildschirm gesperrt
- Dienstliche Unterlagen werden bei Nichtnutzung verschlossen aufbewahrt
- Haushaltsangehörige haben keinen Zugriff auf dienstliche Geräte und Benutzerkonten
- Papierunterlagen werden datenschutzgerecht vernichtet

Geplante Maßnahmen:

- Sicherheitsschlösser

Weitere Maßnahmen:

Passwortschutz aller verwendeten Arbeitsgeräte Automatische Bildschirmsperre bei

Inaktivität Entsperrung der Arbeitsgeräte mittels Passwort, PIN und/oder Face ID

Verwendung individueller, nicht gemeinsam genutzter Benutzerkonten Sichere

Aufbewahrung der Arbeitsgeräte im privaten Homeoffice Kein Zugriff auf Arbeitsgeräte durch unbefugte Personen

3. Zugangskontrolle / Zugriffskontrolle

Alle Maßnahmen, die geeignet sind, die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern sowie alle 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.

Umgesetzte Maßnahmen:

- Login mit Benutzername + Passwort
- Login mit biometrischen Daten
- stets aktueller Virenschutz
- stets aktuelle Softwareversionen
- Verschlüsselter Datentransfer über https/TLS oder vergleichbare Schutzsysteme
- Personal Firewall
- Verschlüsselung von Datenträgern
- Verschlüsselung Smartphones
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablet
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Aktenschredder
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren

Geplante Maßnahmen:

- Richtlinie zum Einsatz von USB-Sticks
- Löschung der Daten wird protokolliert

4. Weitergabekontrolle

Alle 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.

Umgesetzte Maßnahmen:

- Protokollierung der Zugriffe und Abrufe
- Festlegung und Dokumentation der Empfänger
- Daten werden nur an autorisierte Dritte weitergegeben
- Verschlüsselung von Datenträgern und Verbindungen
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
- Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen

Weitere Maßnahmen:

Versand von Informations- und Registrierungsmaterialien Nach Vertragsabschluss wird ein Informationspaket mit Magazinen sowie einer Anleitung zur Registrierung und Nutzung der Online-Bibliothek zusammengestellt und postalisch an den Auftraggeber versandt. Für die Abwicklung des Versands wird die im Rahmen des Vertragsabschlusses angegebene Anschrift des Vertragspartners bzw. Auftraggebers verwendet. Die Adressdaten werden ausschließlich zur Durchführung des Vertrags und zum Versand der zugehörigen Informations- und Registrierungsmaterialien verwendet.

5. Eingabekontrolle

Alle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umgesetzte Maßnahmen:

- Protokollierung von Dateneingaben-, Änderungen und Löschungen
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Klare Zuständigkeiten für Löschungen

Geplante Maßnahmen:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts in Planung
- Administratoren- und Stellvertreterkonzept

6. Auftragskontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Umgesetzte Maßnahmen:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Geplante Maßnahmen:

- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Schriftliche Weisungen an den Auftragnehmer

7. Verfügbarkeitskontrolle / Integrität

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Umgesetzte Maßnahmen:

- Feuer- und Rauchmeldeanlagen
- Technischer Schutz vor Datenverlust und unbefugten Zugriffen durch Virenschutz, Anti-Spyware und Spamfilter

Geplante Maßnahmen:

- Backup & Recovery-Konzept (ausformuliert)
- Ständige Kontrolle des Backup- und Recoverykonzepts

8. Gewährleistung des Zweckbindungs-/Trennungsgebotes

Alle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umgesetzte Maßnahmen:

- Trennung von Produktiv- und Testumgebung
- Steuerung über Berechtigungskonzept
- Datensätze sind mit Zweckattributen versehen