Was sind „TOMs“ (technische und organisatorische Maßnahmen) iSd DSGVO?

Auszug aus Art. 32 DSGVO Sicherheit der Verarbeitung

1. *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 des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahme**n, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
   - *die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;*
   - *die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit der Systeme** und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
   - *die Fähigkeit, die **Verfügbarkeit der personenbezogenen Daten** und den **Zugang** zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
   - *ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*
2. *Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die **Risiken** zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung, Verlust oder Veränderung**, ob **unbeabsichtigt oder unrechtmäßig**, oder **unbefugte Offenlegung** von beziehungsweise **unbefugten Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.*
3. *Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen **unterstellte natürliche Personen**, die Zugang zu personenbezogenen Daten haben, diese **nur auf Anweisung des Verantwortlichen verarbeiten**, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.*

Technische und **organisatorische Maßnahmen**, die dazu dienen, die personenbezogenen Daten vor Verlust oder Zugriff durch unbefugte Personen zu schützen, sind zu **dokumentieren** und auch zu **beschreiben**.

Die angeführten Kategorien (1 – 10) stellen eine Möglichkeit dar, dass sich jede Organisation einen Überblick über die Maßnahmen verschafft; in den einzelnen Punkten finden sich **Vorschläge** für Maßnahmen, die ergänzt bzw. adaptiert werden sollten.

Die unterschiedlich angeführten Maßnahmen können für mehrere Bereiche maßgeblich sein, so z.B. die Benutzeridentifikation oder Protokollierungen.

Die Maßnahmenbeschreibung in der jeweiligen Kategorie stellt ein Beispiel dar, das vom Verwender auf die individuellen Bedürfnisse anzupassen ist.

Auf **www.it-safe.at** (der Wirtschaftskammer Österreich) finden sich Links auf unterschiedliche Dokumente zu technischen und organisatorischen Maßnahmen für KMU und EPU; diese sind sehr hilfreich im Umgang mit personenbezogenen Daten und können eine Anleitung darstellen.

Dieses Dokument stellt lediglich **Anhaltspunkte für technische und organisatorische Maßnahmen** dar, und ist jedenfalls an die **Gegebenheiten der Organisation** und das **Risiko**, das sich aus der Verarbeitung der personenbezogenen Daten durch die Organisation für die betroffenen Personen ergibt, **anzupassen** und zu **ergänzen**.

1. **Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)**

Es soll sichergestellt werden, dass nur berechtige Personen Zugang zu den Anlagen (PC, Laptop, Server …) haben, mit denen personenbezogene Daten verarbeitet werden.

Maßnahmenbeschreibung:
Die Eingangstüre und die Türe zu den Räumen, in denen sich Verarbeitungsanlagen (PC, Server, Laptop, Drucker, Kopierer) befinden, und in denen Akten und Korrespondenz aufbewahrt werden, sind bei Nicht-Benutzung versperrt. Der Serverraum ist versperrt.

Der Laptop/PC wird in einem versperrten Kasten verwahrt.

Der Zutritt zum Serverraum wird protokolliert und es sind nur diejenigen Personen zutritts- bzw. zugriffsberechtigt, die dazu von der Leitung berechtigt wurden

bauliche Maßnahmen zur Verhinderung des physischen Zugangs zu den Verarbeitungsanlagen**:**

- Gebäudesicherung:
- versperrte Eingangs- und Innentüren
- Einbruchssicherung
- Zutrittskontrollsysteme
- Videoüberwachung

technische Maßnahmen, dh Maßnahmen die den „Zugang zum Informationssystem“ regulieren:

- Verfahren zur User-Anmeldung und Abmeldung
- Verwaltung von Admin-rechten
- technische Passwortvorgaben

organisatorische Maßnahmen:

- Besucher werden am Betriebsgelände nicht unbeaufsichtigt gelassen
- eigene Besprechungszimmer, in denen keine Akten zugänglich sind
- Protokollierung über Besuche (wer, wann, bei wem, warum)

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle)

Es soll sichergestellt werden, dass Datenträger, dh Speichermedien, Festplatten etc **nur von berechtigen Personen** verwendet werden können und ein Zugriff auf die Geräte von unbefugten Personen unterbleibt.

Maßnahmenbeschreibung:
Die personenbezogenen Daten sind ausschließlich auf dem einem bestimmten Laufwerk des Servers/Laptop/PC gespeichert, der im .. [Bezeichnung: z.B. xxx] verwahrt wird / im Serverraum steht. Wenn Datenträger entsorgt werden, sichergestellt, dass die darauf befindlichen Daten gelöscht sind.

technische Maßnahmen:

- sichere Aufbewahrung der Speichermedien (versperrt)
- Dokumentieren und Kontrollieren der Anfertigung von Kopien
- verschlüsseltes Speichern
- datenschutzgerechte Entsorgung von Geräten mit Speichermedien (z.B. auch Druckern)
- datenschutzgerechtes Löschen und Wiederverwenden von Speichermedien (Sticks)

organisatorische Maßnahmen:

- Dokumentation der Ausgabe und Verwendung von mobilen Speichermedien (Wer hat welchen USB-Stick oder sonstiges Speichermedium? Nummerierung und Zuordnung)
- Kontrolle über die Datenweitergabe

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

Es soll sichergestellt werden, dass nur befugte (zuständige) Personen die Möglichkeit haben, personenbezogene Daten zu verarbeiten und auf diese zuzugreifen, um diese zu manipulieren.

Maßnahmenbeschreibung:
Die personenbezogenen Daten sind nur von Berechtigten mit Passwort zugänglich. Zugriffe werden protokolliert (need to know). Die Daten werden überdies verschlüsselt abgelegt

technische Maßnahmen:

- Bildschirm- und Computersperre bei Verlassen des Arbeitsplatzes
- Benutzeridentifizierung
- Protokollierung des Verhaltens des Nutzer
- Verschlüsselte Speicherung der Daten
- Trennung von Administration- und Produktionsbereich

organisatorische Maßnahmen:

- Protokollierung der Art und Weise des Zugriffes auf die Daten

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

Es soll sichergestellt werden, dass durch die Verwendung von Verarbeitungssystemen (zB über das Internet) nicht unbefugt Daten übertragen werden.

Der IT-Administrator vergibt die Benutzerrechte im Rahmen des Notwendigen (need to know Prinzip, dh es können nur Befugte auf Daten zugreifen).

Durch technische Systeme (Firewall) und Passwortvorgaben sowie Protokollierung wird sichergestellt, dass Daten nur durch berechtigte Personen übertragen werden.

technische Maßnahmen:

- Firewall, Intrusion Detection/Prevention
- Benutzeridentifizierung
- sichere technische Passwortvorgabe
- Absicherung der Geräte und Netzwerke

organisatorische Maßnahmen:

- Festlegung der Personen, die Nutzungsberechtigungen haben (Zuständigkeiten)
- Protokollierung der Nutzer und Aktivitäten
- Passwortpolicy / Passwortrichtlinie
- Clean-Desk-Policy

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle)

Es soll durch Zuständigkeitsregelungen sichergestellt werden, dass berechtige Personen nur auf die Daten Zugriff haben, für die sie auch berechtigt sind.

Es besteht eine Passwort-Policy und diese ist den Befugten auch bekannt. Passwörter sind in periodischen Abständen zu ändern. Es ist sichergestellt, dass alle befugten Personen informiert sind, dass Passwörter sicher zu verwahren sind und nicht weitergegeben werden. Die befragten Personen sind informiert, dass einzigartige Passwörter, dh Passwörter, die vom Nutzer bei keinem anderen (insbesondere privaten) Systemen verwendet werden sollen.

technische Maßnahmen:

- Berechtigungskonzept
- Benutzeridentifizierung
- Schnittstellensicherung
- Verschlüsselung
- Kopierkontrolle
- Netzwerkkontrolle (kein Anschluss von nicht betriebseigenen Geräten)
- Berechtigungsprüfung (automatisiert)

organisatorische Maßnahmen:

- Verwaltung und Kontrolle der Zugriffsberechtigungen
- Kontrolle der Zugriffe (Protokollierung)
- Dokumentation der Maßnahmen zur Datenvernichtung

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)

Es soll sichergestellt werden, dass Daten im Rahmen der Übertragung nur an berechtigte Empfänger übermittelt werden.

Daten werden nur an berechtigte Empfänger (z.B. Auftraggeber im Rahmen der Geschäftsbeziehung, Banken im Rahmen des Zahlungsverkehrs) elektronisch übertragen.

Bei Verwendung der Daten für Schriftstücke gibt es ein Vier-Augen-Prinzip.

Wenn Daten per Email übermittelt werden, dann erfolgt das in einem Anhang zum Email und der Anhang ist passwortgeschützt sowie ist das Passwort nur dem berechtigten Empfänger bekannt. Es ist in einer Richtlinie festgelegt, an welche Empfängerkategorien Übermittlungen erfolgen.

technische Maßnahmen:

- Protokollierung von Datenübermittlungen
- Auswertungsmöglichkeiten (Feststellung der Sender und Empfänger)

organisatorische Maßnahmen:

- Festlegung von Übermittlungswegen (wie wird an welche Empfängerkategorie übermittelt)

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle)

Es soll die Nachvollziehbarkeit sichergestellt werden.

Es wird - wenn mehrere Benutzer auf Systeme und personenbezogene Daten zugreifen können - mitprotokolliert, welcher Benutzer auf welche Daten zu welchem Zeitpunkt zugegriffen hat. Diese Protokolle stehen der IT-Administration zur Verfügung und werden nur im Anlassfall (zB. bei

technischen Beeinträchtigungen oder aus datenschutzrechtlichen Gründen) eingesehen. Die Protokolle werden in angemessenen periodischen Zeiträumen gelöscht.

technische Maßnahmen:

- Benutzeridentifizierung
- Protokollierung der Eingabe, Änderung und Löschung von personenbezogener Daten
- Einsatz von elektronischen Signaturen

organisatorische Maßnahmen:

- Festlegung von Berechtigungen
- sichere Ablage und fristgerechte Löschung von Protokollen

8. Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle)

Es soll sichergestellt werden, wenn Daten übermittelt oder auf Datenträgern transportiert werden, diese auch beim berechtigen Empfänger ankommen.

Es besteht die Weisung, dass Daten nicht auf mobilen Datenträgern gespeichert werden (USB-Sticks, Smartphones).

Der Laptop/PC darf nur von befugten Personen verwendet und transportiert werden.

Wenn der Laptop oder PC z.B. zur Reparatur außer Haus gebracht wird, ist sichergestellt, dass der Empfänger die Daten vertraulich behandelt (vertragliche Regelung)

technische Maßnahmen:

- Verschlüsselte Übertragung und Speicherung auf Datenträgern
- Zugriff mittels verschlüsselten VPNS
- Protokollierung der Übermittlung von Daten
- Duplizieren von Datenträgern
- Schutz vor Schadsoftware (z.B. Viren)

- sicheres Löschen auf Datenträgern
- Verwendung von sicheren Transportbehältern

organisatorische Maßnahmen:

- Sicherstellung von sicheren Transporten von Datenträgern (zuverlässige Personen oder Unternehmen)
- Kontrolle des Transportweges und der Transportzeit (Rückfrage)
- Datenträger-Eingangs- und Ausgangsverzeichnis

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellung)

Es soll sichergestellt werden, dass die IT-Systeme nach einem Zwischenfall möglichst rasch – mit den personenbezogenen Daten – wiederhergestellt werden können.

Es besteht eine Sicherung der Daten (Form der Sicherung: …, zeitlicher Abstand der Sicherung: …). Die IT-Administration ist in der Lage, die Sicherung zeitnahe einzuspielen; das Szenario wird in periodischen Abständen getestet

technische Maßnahmen:

organisatorische Maßnahmen:

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

Es soll sichergestellt werden, dass es durch Fehlfunktionen keine Beeinträchtigungen an den personenbezogenen Daten gibt.

Es erfolgen die notwendigen Updates des Betriebssystems und der sonstigen Programme.

Es gibt einen ausreichend Schutz gegen Intrusion und Viren.

technische Maßnahmen:

- Datensicherungen erfolgen in periodischen Abständen
- Einsatz von Virenscannern, Firewalls, Spam-Filter)
- Sicherstellung der Stromversorgung bei Ausfall
- Einsatz von elektronischen Signaturen

organisatorische Maßnahmen:

- Datensicherungs- und Wiederherstellungskonzept
- Systemüberwachung der relevanten Hard- und Software

www.dataprotect.at
SMP Schweiger Mohr & Partner Rechtsanwälte OG
Huemerstraße 1 / Kaplanhofstraße 2, A-4020 Linz
ATU 40112014 Tel 0732/79 69 00 Fax 0732 796906
FN 37294w LG Linz / Österreich

Verfasser: RA Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E