# Technisch organisatorische Maßnahmen (ToM)

## Was sind technisch organisatorische Maßnahmen (TOM)?

Um personenbezogene Daten in Unternehmen zu verarbeiten, muss sichergestellt sein, dass diese Daten vor unberechtigtem Zugriff geschützt sind. Dazu schreibt der Gesetzgeber seit dem 23.5.2018 im Rahmen der DSGVO vor, ToM umzusetzen. Jeder Verantwortliche hat die TOM in seinem Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren.

Entgegen vorheriger Regelungen handelt es sich jetzt um ein Gesetz, nicht um eine Empfehlung und kann bei Nichteinhaltung Strafen bis zu 20% des Jahresumsatzes nach sich ziehen.

Durch Umsetzung geeigneter TOM soll dies sichergestellt werden. Dabei handelt es sich um Vorkehrungen, die von Verantwortlichen im Unternehmen oder einem beauftragten IT-Dienstleister getroffen werden, um die Sicherheit der erhobenen und verarbeiteten personenbezogenen Daten im Rahmen der DSGVO zu garantieren.

Die Grundsätze des Datenschutzes geben vor, durch Technik und datenschutzbezogene Einstellungen (Privacy by Default und Privacy by Design) diese Grundsätze nach stets aktuellem Stand der Technik umzusetzen. Dazu müssen gem. Art. 32 Abs. 1 DSGVO unter anderem folgende Maßnahmen ergriffen werden:

- 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 Verfügbarkeit der personenbezogenen Daten
- Wiederherstellung des Zugangs zu den personenbezogenen Daten bei einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

## Zu welchem Zweck müssen TOM umgesetzt werden?

TOM sollen sicherstellen, dass personenbezogene Daten dem neusten Stand der Technik nach ausreichend geschützt, gesichert und wiederherstellbar sind. Ratsam ist, im Vorfeld mit einem Experten eine Risikoanalyse zu erstellen, um sicherzustellen, dass alle im Unternehmen gespeicherten und verarbeiteten personenbezogenen Daten auch hinsichtlich bestehender Risiken ausreichend geschützt werden.

Für die Praxis bedeutet das:

Alle gesetzlich vorzuhaltenden Daten müssen nach einem technischen Zwischenfall unkompliziert wiederherstellbar sein. Computer und Festplatten sind Verschleißteile. Werden durch einen Defekt Daten zerstört, muss weiterhin sichergestellt sein, dass alle vorzuhaltenden Daten in einem oder mehreren, auch dezentralen, Backups vorliegen. Dazu gehören nicht nur personenbezogene Daten, sondern auch Steuerunterlagen, Handwerkerrechnungen oder geschäftliche Kommunikation im Rahmen von zustandegekommenen Projekten und Abrechnungen, die einer Archivierungs- und

Löschfrist unterliegen.

Die Zeiten, wo man sich vom Finanzamt schätzen lassen konnte, wenn Unterlagen nicht mehr vorhanden waren sind vorbei und heute bedeutet es Strafe nach DSGVO.

## Achtung! Meldepflicht!

Mit dem Thema Datensicherung hat es zwar nur indirekt zu tun, kommt aber in den Fällen zum Tragen, wenn man seine Daten beispielsweise auf einen externen unverschlüsselte Datenträger kopiert und diese beim Transport nach Hause, verlorengeht. Hier muss ich ganz klar vor derart unprofessionellen Lösungen warnen! Die Strafen kosten ein vielfaches von der Investition in ein professionelles Konzept und eine gute Begleitung.

Aber ich möchte in diesem Rahmen darauf hinweisen, dass für den Fall, dass personenbezogene Daten in dieser oder irgendeiner Form nach Außen gelangen, also eine eine Datenpanne passiert, sofort zu handeln ist! Hier sieht der Gesetzgeber eine Meldepflicht in Art. 33 DSGVO vor. Darin ist festgelegt, dass die Meldung eines Verstoßes **innerhalb von 72 Stunden** zu erfolgen hat. Hierbei bedeutet 72 Stunden exakt 72 Stunden nach bekanntwerden der Panne ohne Rücksicht auf Sonn- und Feiertage.

Eindeutige ID: #1400
Verfasser: KP
Letzte Änderung: 2021-11-26 12:24