Up to Data:
Technische und organisatorische Maßnahmen

Wer sich mit dem Datenschutz in seinem Unternehmen beschäftigt, kommt nicht umhin, sich auch mit den sog. technischen und organisatorischen Maßnahmen (kurz: TOM oder TOMs) zu beschäftigen.

Was sind TOMs überhaupt?

Die Notwendigkeit der Umsetzung von bestimmten TOMs ergibt sich aus Art. 24 Abs. 1 S. 1 DSGVO. Hier heißt es:

*Der **Verantwortliche** setzt unter Berücksichtigung der **Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung** sowie der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen** geeignete **technische und organisatorische Maßnahmen** um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.*

TOMs sind also diejenigen Maßnahmen, die im Rahmen der technischen oder organisatorischen Überprüfung des Unternehmens vorgenommen werden, um sicherstellen zu können, dass ein Datenverlust nahezu ausgeschlossen ist. Art. 32 DSGVO gibt dabei erste Anstöße, was man konkret unter den technischen und organisatorischen Maßnahmen verstehen kann. Beispielsweise (und nicht abschließend) wird dort die Pseudonymisierung oder die Verschlüsselung personenbezogener Daten aufgelistet. Auch geht es bei der Bereitstellung der TOMs um die Herstellung eines generellen Schutzniveaus im gesamten Unternehmen.

Zusammenfassung im Überblick

	Technische Maßnahmen	Organisatorische Maßnahmen
Beschreibung	Die technischen Maßnahmen haben Einfluss auf die technische Datenverarbeitung. Hierunter fallen alle Maßnahmen, die die Sicherheit der eingesetzten IT-Systeme oder die Sicherheit des Gebäudes an sich betreffen.	Die organisatorischen Maßnahmen bilden und beeinflussen die Rahmenbedingungen der technischen Verarbeitung.
Beispiele	- Verschlüsselung von E-Mails oder Datenträgern - Einsatz von Virenprogrammen und einer Firewall - Datensicherungen und automatische Backups	- Zugangs- und Zutrittskontrolle /-beschränkungen - Festlegung von Berechtigungskonzepten für Personengruppen

	- Glasbruchmelder, Alarmanlagen	- Schulung der Mitarbeiter im Datenschutz - Vier-Augen-Prinzip

Welche TOMs sind angemessen für unser Unternehmen? – Das ZAWAS-Prinzip

Wahrscheinlich fragen Sie sich als Leser nun, welche technischen und organisatorischen Maßnahmen Sie in Ihrem Unternehmen umsetzen müssen. Dies kann man jedoch konkret gar nicht sagen. Jedem Unternehmen steht ein sog. Auswahlermessen zu, welches sich aus mehreren Kriterien ergibt. Dazu zählt der Stand der Technik im Unternehmen, Implementierungskosten, die Eintrittswahrscheinlichkeit und die Schwere des Risikos für Rechte und Freiheiten der Betroffenen, sowie Art, Umfang, Umstände und Zweck der Verarbeitung. Jedes Unternehmen muss also seinen eigenen, auf das Unternehmen zugeschnittenen, Maßnahmenkatalog entwickeln.

Zur Auswahl der TOMs hat die Landesbeauftragte für den Datenschutz (LfD) in Niedersachen einen Prozess **z**ur **A**us**w**ahl **a**ngemessener **S**icherheitsmaßnahmen entwickelt („ZAWAS"-Prinzip). Sie will dadurch Unternehmen eine Hilfestellung für die Umsetzung der TOMs geben. Dieser Prozess ist geeignet, die entsprechenden TOMs systematisch herzuleiten.

Nachfolgend haben wir Ihnen die Methodik zusammengefasst. Die ausführliche Folienpräsentation der LfD können Sie bei Interesse unter dem Link[1] nachlesen.

1. ***Verarbeitungstätigkeit beschreiben***
   Fassen Sie zusammen, welche Zwecke mit der Verarbeitung verfolgt werden, welche Daten die Verarbeitung betrifft und beschreiben Sie den Ablauf der Verarbeitung.

2. ***Rechtliche Grundlagen prüfen***
   Stellen Sie sicher, dass die Verarbeitung auf einer zulässigen Rechtsgrundlage basiert und die Grundsätze der DSGVO eingehalten werden. Denn: Ohne Rechtsgrundlage keine rechtmäßige Datenverarbeitung!

3. ***Strukturanalyse durchführen***
   Ermitteln und beschreiben Sie die zu schützenden Objekte der Verarbeitungstätigkeit. Geben Sie außerdem deren Beziehung zueinander an. Zum Beispiel die IT-Systeme, das Gebäude oder spezifische Räume.

[1] https://www.lfd.niedersachsen.de/startseite/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html – Stand 25.06.2020

4. ***Risiken identifizieren und Schadenswerte einschätzen***
   Bestimmen Sie Ereignisse, die zu einem Schaden führen können und bestimmen Sie den Schadenswert des Risikos anhand der Eintrittswahrscheinlichkeit und der Schwere des Risikos. (z.B. Datenpanne durch Hackerangriff)

5. ***Maßnahmen auswählen***
   Suchen Sie unter Berücksichtigung der oben genannten Kriterien nach geeigneten Maßnahmen, um die identifizierten Risiken einzudämmen. Achten Sie dabei auf die bestimmten Schadenswerte und wählen Sie geeignete Maßnahmen zur Prävention aus. Sie können sich am IT-Grundschutz-Kompendium, oder an den Maßnahmen des Standard-Datenschutzmodells orientieren.

6. ***Restrisiko bewerten***
   Ermitteln Sie die bestehenden Restrisiken, wenn die nach Punkt 5 ausgewählten Maßnahmen implementiert wären. Sollte weiterhin ein hohes Risiko bestehen, müssen Sie neue Maßnahmen bestimmen, oder den Verarbeitungsprozess anpassen.

7. ***Maßnahmen konsolidieren***
   Hierbei sollen nun alle Maßnahmen als Einheit betrachtet werden. Es kann sein, dass Maßnahmen überflüssig sind, weil eine andere Maßnahme ein besseres Schutzniveau gewährleistet. Konkretisieren Sie außerdem Maßnahmen, wenn bei der Gesamtbetrachtung das Ziel der Maßnahme nicht klar ist.

8. ***Maßnahmen realisieren***
   Verteilen Sie Aufgaben und Verantwortlichkeiten und priorisieren Sie bei Budget- bzw. Personalknappheit Ihre Maßnahmen. Setzen Sie nun die festgelegten Maßnahmen um.

Was ist für das Jahr 2020 und 2021 zu erwarten?

Nachdem die DSGVO seit nunmehr zwei Jahren für uns alle gilt, liegt die Vermutung nahe, dass in naher Zukunft vermehrt die **TOMs** und der Inhalt von **Verarbeitungsverzeichnissen** durch die Aufsichtsbehörde geprüft wird.

Die RKM Data empfiehlt also, sich in diesem und im nächsten Jahr verstärkt mit der Aktualisierung der Verarbeitungsverzeichnisse und der Entwicklung geeigneter Sicherheitsmaßnahmen zu beschäftigen.

Wichtig ist hier, dass eine nachvollziehbare Dokumentation über die TOMs erfolgt.

Gern können Sie sich bei Fragen zu diesen Themenkomplexen an uns wenden!

Ihr Team der RKM Data GmbH