Mega-Strafe wegen Verletzung der TOMs: Was lernen wir daraus?

Haben Sie alles DSGVO-konform erfüllt?

Im **Juni-BAV-Newsletter** brachten wir einen kurzen Rückblick auf die **wichtigsten Urteile**, die von den diversen Datenschutzbehörden getroffen wurden und fragten, ob Sie im eigenen Unternehmen schon alle Hausaufgaben erfüllt haben oder noch etwas erledigen müssen, weil sich etwa in den letzten Monaten etwas verändert hatte?
Auch gaben wir den wichtigen Hinweis darauf, dass Ihnen **Schadenersatz-Klagen drohen** könnten. Eine Gefahr, die durch eine oberstgerichtliche deutsche Entscheidung sogar noch größer wurde.

Und schließlich erstellten wir ein **„1x1 des Datenschutzes", also die wichtigsten Punkte,** die man auf jeden Fall erfüllen muss.

Im heutigen zweiten Teil unseres Beitrags zur DSGVO sehen wir uns die TOMs, näher an.
Denn eine der **höchsten bisher ausgesprochenen DSGVO-Strafen** hat die **portugiesische Datenschutzbehörde** über ein Spital verhängt, weil die Behörde **Verfehlungen bei den TOMs, also den technischen und organisatorischen Maßnahmen,** die im Zuge der DSGVO-Umsetzung realisiert werden mussten, feststellten.

Konkret musste das Unternehmen **400.000 Euro** bezahlen. Die Strafe war nur **deshalb „so" gering,** weil man sich kooperativ gegenüber der Behörde zeigte und aktiv an der Behebung der Mängel mitgearbeitet wurde. Dennoch musste diese Strafe tatsächlich bezahlt werden.

Diese Mega-Strafe sollte Motivation genug sein, um sich die Anforderungen der DSGVO bezüglich der **TOMs in Erinnerung zu rufen.** Und zu checken, ob man nun – also rund drei Jahre nach Start der DSGVO – hier nicht nachbessern sollte.

In vielen Unternehmen wird **auf die TOMs vergessen oder man beschäftigte sich kurz und oftmals halbherzig mit dem Thema,** in dem man glaubte, man lädt sich das Standard-Formular dazu herunter und vergisst jedoch, dass dieser Text dann individuell gestaltet werden muss. D.h. die Textbausteine des TOM-Dokuments sind auf das Unternehmen anzupassen. Es gilt genau zu **beschreiben,** welche „technischen und organisatorischen Maßnahmen" – das versteckt sich unter dem Begriff „TOM" – man im eigenen Haus erarbeitet und umgesetzt hat.

Tipp: Dieses „TOM-Dokument" sollte man nun, 3 Jahre nach dem Ablauf der Schonfrist der DSGVO, kontrollieren, ob es nach wie vor passt (oder man neue Maßnahmen eingeführt hat) bzw. prüfen, ob die damals beschlossenen Maßnahmen auch wirklich befolgt werden.

Klar ist: Die TOMs scheinen in der **Praxis für viele Unternehmen schwierig umzusetzen**, weil es sich dabei oftmals um (EDV-)technische Anforderungen und Maßnahmen zur EDV-/IT-Sicherheit handelt, die besonders bei Klein- und Mittelbetrieben zu großen Schwierigkeiten führen. Daher wollen wir das Thema nun **näher beleuchten und Ihnen Hinweise und Tipps für die tägliche Praxis dazu geben.**

Konkret informieren wir heute darüber, was genau man **unter den TOMs versteht** und worin die Unterschiede zwischen **Zutritts-, Zugangs- und Zugriffskontrolle** bestehen und bringen typische Umsetzungs-Beispiele dafür.

TOM ist die Abkürzung für „**T**echnische und **O**rganisatorische **M**aßnahmen".

Definiert werden die technischen und organisatorischen Maßnahmen, die Sie setzen müssen, im **Artikel 32 der DSGVO.** Sowohl **Verantwortliche, aber auch Auftragsverarbeiter** haben dafür zu sorgen, dass „geeignete technische und organisatorische Maßnahmen" implementiert sind, die sicherstellen, dass „ein angemessenes Schutzniveau gewährleistet ist".

Diese TOMs sollen sicherstellen, dass die **Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit** der Daten und damit der Systeme gegeben ist.

Wichtig: Sie als Unternehmer (und damit als **Datenverantwortlicher)** müssen für Ihre Kunden und Partner die Sicherheit der Daten im System garantieren. Aber Sie müssen sich auch von jedem Ihrer **Auftragsverarbeiter** (z.B. Druckerei, die für Sie ein Mailing versendet) bestätigen lassen, dass dieser TOMs hat und diese auch befolgt.

Für den Verantwortlichen sind dabei der Stand der Technik, die Implementierungskosten und das Risiko (Eintrittswahrscheinlichkeit und Schadenshöhe) zu berücksichtigen.

Heute sehen wir uns **4 der insgesamt 8 Kontroll-Bereiche** näher an und geben Tipps für die Praxis. **Die restlichen 4 folgen** dann im nächsten BAV-Newsletter.

Zutritts-, Zugangs- und Zugriffs- sowie Weitergabekontrolle sind wichtige Maßnahmen, um Datenschutz und Datensicherheit herstellen zu können.

Wo liegen die Unterschiede?

1. Die **ZUTRITTS**kontrolle soll sicherstellen, dass keine unbefugten Personen zu Gebäuden, Räumen, EDV-Anlagen, Computer, Drucker, FAX etc. und damit zu personenbezogenen Daten – Zutritt haben.

Mögliche Maßnahmen zur Umsetzung könnten sein: Videoüberwachung, Alarmanlage, Wachdienst, Portier oder andere Form der Gebäudesicherung/Personenkontrolle, Chipkarten-Lösung, einbruchssichere Türen und Fenster, versperrbare Räume und Schränke, usw.

Was auch immer Sie in Ihrem Unternehmen diesbezüglich einsetzen: **Beschreiben Sie das in Ihren TOMs,** um zu dokumentieren, was Sie tun, um unbefugte Kenntnis- oder Einflussnahme von Daten auszuschließen. Je sensibler die Daten, umso besser sollten Ihre Schutzmaßnahmen sein. Finanzdaten sind schon heikel, ganz besonders schutzbedürftig sind jedoch Gesundheitsdaten (die man z.B. im Zuge von Lebensversicherungen, etc. erhalten hat).

2. Die **ZUGANGS**kontrolle soll verhindern, dass Unbefugte Hard- und Software nutzen können.
Die Zutrittskontrolle soll den physischen Zutritt verhindern, die Zugangskontrolle soll die Nutzung der Systeme verhindern.

Mögliche Maßnahmen zur Umsetzung könnten sein: PC und besonders Laptops mit Bildschirmschoner und Passwortschutz versehen, Passwortrichtlinie (wie sehen sichere Passwörter aus?), Liste mit Benutzernamen und Passwörtern (wer hat Zugriff auf was? **Beim Ausscheiden von Mitarbeitern** sind Zugänge sofort zu deaktivieren), PIN-Vergabe, Nutzung von Spamfilter, Virenscanner, Firewalls, laufend aktualisierte Software, etc.

Tipp: Heutzutage sind besonders die Angriffe von außen über das Internet eine zunehmende Gefahrenquelle und ein bedeutendes Einfallstor für Cyberkriminelle und Datendiebe. Daher sind auch auf Servern sichere Passwörter, besondere Admin-Rechte und das Aufzeichnen von Zugriffen, etc. von größter Bedeutung.

3. Die **ZUGRIFFSkontrolle** soll sicherstellen, dass keine Unbefugten Zugriff auf personenbezogene Daten, Programme, und Dokumente erhalten, obwohl sie bereits in das Gebäude gelangt sind und Zugriff auf PC/Laptop erhalten haben.
Je nach Aufgabenbereich sollte es unterschiedliche Berechtigungen geben. Nicht jeder darf alles. Mitarbeiter der Personal-Abteilung haben Zugriff auf ganz andere Daten, als die der Marketing-Abteilung.
DAS war einer der **Kritik-Punkte der Behörde** bei der oben zitierten Mega-Strafe gegen das Portugiesische Krankenhaus.
Und auch die Tatsache, dass beim Ausscheiden von Mitarbeitern die Zugriffsmöglichkeiten nicht sofort deaktiviert wurden, war heftig kritisiert worden.

In Großbetrieben wird wohl im Zug eines Berechtigungskonzeptes ersichtlich sein, wer auf welche Server, Programme, Daten Zugriff hat. Aber auch in Klein-Unternehmen sollte es eine Liste geben, aus der ersichtlich ist, wer unter welchen Benutzernamen worauf Zugriff hat.

Tipp: Besonders beim Einsatz von **mobilen Geräten** (Handy, Laptop, USB-Sticks, Kamera, etc.) und **technischen Möglichkeiten** (E-Mail, WhatsApp, etc.) ist hier besonders aufzupassen.

Mögliche Maßnahmen zur Umsetzung könnten sein: Erstellen eines Berechtigungskonzeptes, Vergabe von Admin-Rechten, Konzept und Arbeitsanweisung für die Nutzung mobiler Geräte, Einrichtung von sicheren Kommunikationsmöglichkeiten (E-Mail-Verschlüsselung, Dateien vor Versand mit Passwort versehen, etc.), Vorgabe von Verschlüsselung für Geräte (etwa Bitlocker am PC aktivieren, USB-Sticks, etc.), verschlüsseltes WLAN, usw.

Aber auch für das **Ausscheiden und Vernichten von Datenträgern und Hardware** sollte es eine DSGVO-konforme Vorgabe geben, die auch immer wieder überprüft wird.

Sie sehen aus obiger Aufzählung, dass sich Zutritts-, Zugangs- und Zugriffskontrolle oftmals **schwer voneinander abgrenzen lassen, oftmals nahtlos ineinander greifen.**

Das Ziel ist aber immer: Ein unbefugtes Lesen, Kopieren, Verändern oder Löschen personenbezogener Daten sollte unbedingt verhindert werden.

Auf jeden Fall sollte man viele Maßnahmen setzen, um dieses Ziel zu erreichen. Und diese auf jeden Fall auch dokumentieren, um der Behörde das Bemühen beweisen zu können.

4. Die **WEITERGABEkontrolle** soll sicherstellen, dass keine Daten an Unbefugte weitergeben werden. Diese Weitergabe kann beabsichtigt oder unabsichtlich passieren.
Daher sollten Sie vorher klären, ob Sie jemand wirklich Daten etwa bei Anfragen weitergeben dürfen.
Unabsichtlich können Daten in falsche Hände geraten, weil etwa E-mails abgefangen oder mitgelesen werden.

Daher sollten etwa VPN-Tunnel-Software (vor allem wenn man außerhalb des EDV-geschützten Büros arbeitet), verschlüsselte E-mails oder mit Passwort-gesicherte Dokumente standardmäßig zum Einsatz kommen.

Wichtig: Es ist nötig, regelmäßig die Mitarbeiter an die Pflichten aus der DSGVO zu erinnern und sie auch entsprechend zu schulen, wenn man Mängel feststellt.

Im nächsten BAV-Newsletter sehen wir uns die **weiteren 4 TOMs-Bereiche** näher an. Also Eingabe- , Auftrags-, Verfügbarkeits- und Datentrennungskontrolle.

Weiters informieren wir über das **ordnungsgemäße Vorgehen, wenn doch etwas passiert**, also ein „Data breach" eingetreten ist.

Für weitere Rückfragen:

RA Mag. Stephan Novotny

1010 Wien, Weihburggasse 4/2/22
kanzlei@ra-novotny.at
https://www.ra-novotny.at

Foto: Stephan Huger

Quellen und Mitarbeit: Mag. Stephan Novotny (https://www.ra-novotny.at/), Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche (www.b2b-projekte.at), Newsletter von meineberater.at, Zurich BAV-Newsletter