DSGVo-Umsetzungs-Tipps für die Praxis:
Was lernen wir aus der Mega-Strafe wegen Verletzung der TOMs?

Im heutigen Praxis-Beitrag sieht sich der auf Versicherungsrecht und DSGVO spezialisierte Jurist Mag. Stephan Novotny **genauer an, warum ein** portugiesisches Spital zu 400.000 Euro **verurteilt wurde.** Und was wir daraus lernen können.

Weiters erklärt Mag. Novotny was genau man **unter den TOMs versteht** und worin die Unterschiede zwischen **Zutritts-, Zugangs- und Zugriffskontrolle** bestehen und bringt typische Umsetzungs-Beispiele dafür.

Einige **Praxis-Tipps** (Windows 7 läuft per 1.1.2020 ab, FMA-IT-Leitlinien, Databreach, etc.) **runden seinen heutigen Beitrag ab.**

Hier folgt nun der Beitrag von Mag. Novotny:

DSGVO-Umsetzungs-Tipps zu den TOMs

Eine der höchsten bisher ausgesprochenen DSGVO-Strafen hat die **portugiesische Datenschutzbehörde über ein Spital** verhängt. 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. Die dortigen **Verfehlungen betrafen die TOMs, also die technischen und organisatorischen Maßnahmen,** die im Zuge der DSGVO-Umsetzung realisiert werden mussten.

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 ein Jahr nach Start der DSGVO – hier nicht nachbessern sollte.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

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, eineinhalb 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.**

Was sind TOMs?

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.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Zutritts-, Zugangs- und Zugriffskontrolle 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 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.

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 mit Bildschirmschoner und Passwortschutz, 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, 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 **ZUGRIFFS**kontrolle soll sicherstellen, dass keine Unbefugten Zugriff auf personenbezogene Daten, Programme, und Dokumente erhalten. **Je nach Aufgabenbereich sollte es unterschiedliche Berechtigungen** Nicht jeder darf alles. **DAS** war einer der **Kritik-Punkte der Behörde** bei der oben zitierten Mega-Strafe gegen das Portugiesische Krankenhaus. Und beim Ausscheiden von Mitarbeitern sind die Zugriffsmöglichkeiten sofort zu deaktivieren. 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.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

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 ineinandergreifen.

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 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.

5. Über die **EINGABEkontrolle** kann **nachverfolgt werden, wer wann Daten ins System eingegeben, verändert, gelöscht** hat. Dadurch kann – zumindest nachträglich – herausgefunden werden, ob und wer Daten manipuliert hat. Deshalb sollten Sie in Ihrem Unternehmen vorab überlegen, wer auf welche Daten wirklich Zugriff benötigt (Nicht allen alles erlauben! Wozu sollte ein Lagerarbeiter auf Lohndaten zugreifen dürfen?).
Durch die **Vergabe von Nutzernamen/Passwort** kann man die Zugriffe genau nachverfolgen. Bereits dieses Wissen um die Nachvollziehbarkeit der Zugriffe wirkt abschreckend und hilft Missbrauch von Daten zu verhindern.

6. **AUFTRAGSkontrolle**
Vorab zum Erinnern: Die TOMs werden im Artikel 32 der DSGVO definiert. 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“.**

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Der **Verantwortliche** ist die Person, das Unternehmen, die/das über die Verarbeitung von personenbezogenen Daten entscheidet. Er ist dafür verantwortlich, dass die Daten der Kunden/Mitarbeiter/Lieferanten etc. bestmöglich geschützt werden.
Der **Auftragsverarbeiter** ist dagegen eine Person/ein Unternehmen, das im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet.
Bei der Auftragskontrolle geht es konkret um die Kontrolle Ihrer Auftragsverarbeiter, um sicherzustellen, dass diese die Daten exakt nach Ihren Weisungen verarbeiten und alles tun, um die Daten zu schützen.

Tipp 1: Gehen Sie Ihre Lieferanten-Liste durch und checken Sie, wer als Auftragsverarbeiter für Sie tätig wird.
Tipp 2: Verlangen Sie von allen Ihren Auftragsverarbeitern regelmäßig deren TOMs, um prüfen zu können, ob diese nach wie vor die DSGVO am Radar haben und Maßnahmen zum Schutz Ihrer Daten und die Ihrer Kunden gesetzt haben. Es ist ein Leichtes für die Datenschutzbehörde zu kontrollieren, ob Sie diese formale Voraussetzung erfüllt haben. Falls nicht, gibt es für Sie nichts zu diskutieren und zu argumentieren …

Ein paar Ideen, wer für Sie als Auftragsverarbeiter tätig ist:
Druckerei (produziert ein Mailing mit Ihren Daten), EDV-Techniker, IT-Dienstleister, Software-Lieferant, Werbeagentur, Cloud-Anbieter …

Ausnahmen: KEINE Auftragsverarbeiter sind – trotzdem sie Ihre Daten verarbeiten: Steuerberater, Wirtschaftsprüfer, Anwälte …
Von diesen Firmen benötigen Sie keinen Auftragsverarbeitervertrag (AVV), weil diese Personen/Firmen als „Berufsgeheimnisträger“ gelten. Bei Steuerberatern kommt noch dazu, dass sie aufgrund ihres Berufsrechts stets weisungsUNabhängig und eigenverantwortlich tätig sind. Während das typische Zeichen für Auftragsverarbeiter ist, dass diese weisungsgebunden sind.

7. VERFÜGBARKEITSkontrolle

Ziel ist, dass die **Daten immer verfügbar** sind und vor einem zufälligen (wegen Irrtum) oder bewussten (etwa durch Hacker-Angriff) **Löschen geschützt sind** oder im Fall des Falles von einem Back-up wiederhergestellt werden können.
Überlegen Sie sich also eine **Backup-Strategie** für Ihr Unternehmen, idealerweise eine automatische und mehrfache Speicherung an unterschiedlichen Orten, um auf Nummer sicher zu gehen. Aber auch technische Vorkehrungen wie eine unterbrechungsfreie Stromversorgung (also USV-Gerät), besondere Feuersicherung (Feuermelder, Feuerlöscher) bzw. Klimageräte im und Zugangskontrolle vor dem Server-Raum können hier wertvolle Hilfe leisten.

8. DATENTRENNUNGSkontrolle

Hier geht es darum, dass **Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden müssen,** also nicht alle Daten eines Kunden zusammengeführt werden dürfen.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Ein Beispiel in diesem Zusammenhang ist, dass Sie eine E-Mail-Adresse, die Sie erhalten haben, um z.B. einen Vertrag für eine Lebensversicherung abzuwickeln, nicht dazu verwenden dürfen, um diesem Kunden eine Werbung für eine Solaranlage, deren Vertrieb Ihr Unternehmen ebenso übernommen hat, via E-Mail zu senden.

Ein Ausweg in diesem Fall wäre die gute alte Post, also ein Brief mit der Information und Übermittlung Ihres Angebotes.
Wahrscheinlich wird es im Falle einer guten Kundenbeziehung beim oben skizzierten Fall kein Problem geben. Aber juristisch betrachtet gilt: Wenn Sie personenbezogene Daten eines Kunden auch für einen anderen Zweck verwenden wollen, brauchen Sie eine entsprechende Rechtsgrundlage. Also die aktive Einwilligung des Kunden, dass Sie seine E-Mail-Adresse für den Newsletter mit allen möglichen Produkten Ihres Unternehmens verwenden dürfen.

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.

Abschließende Tipps für heute:

*) Wenn es zu einem **Data breach** (also Einbruch mit möglichen Datenverlust) gekommen ist, ist das dafür vorgesehene Procedere abzuarbeiten und die Behörde zu informieren. Darüber berichten wir im nächsten Newsletter.

*) Um die Folgen eines technischen Problems oder eines Hackerangriffs möglichst gering zu halten, ist unbedingt ein **Speicherkonzept** zu erstellen und zu befolgen (**regelmäßige Speicherung** Ihrer Daten auf verschiedenen Medien an verschiedenen Orten und ein **Verfahren für den GAU** (größtmöglich anzunehmender Unfall, etwa Hackerangriff) und das Wiederherstellen der Daten und das Informieren der Datenschutzbehörde und aller Betroffenen definieren und dokumentieren.

*) **Auf IT und EDV schaut die Behörde ganz genau.** Bedenken Sie in diesem Zusammenhang, dass per **1.1.2020 Windows 7 abläuft,** d.h. von Microsoft nicht mehr mit Updates versorgt wird. Sollten Sie dieses Betriebssystem also immer noch nutzen, schauen Sie sich rechtzeitig um eine Alternative umsehen.

Denn passiert Ihnen ein Hacker-Angriff oder ein anderes Datenleck, könnte Ihnen die Behörde vorwerfen, dass Sie wegen dem dann unsicher gewordenen System am Datenverlust (mit-) schuld sind.

*) Die **FMA hat IT Leitlinien** für die unterschiedlichen Branchen veröffentlicht. Schauen Sie sich an, was die Behörde sich hier von Ihnen erwartet. **Zum Nachlesen** hier klicken…

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

*) Finaler Tipp für heute: Die **Adresse der Datenschutzbehörde hat sich geändert.** Viele von Ihnen haben sie aber in Formularen oder auf Webseiten stehen. Daher sollte das geändert werden.

Neue Adresse der DSB lautet:
Österreichische Datenschutzbehörde
Barichgasse 40-42
1030 Wien
Telefon: +43 1 521 52-25 69
E Mail: dsb@dsb.gv.at

Quellen: Homepage der Datenschutzbehörde, Computermagazin Chip.de, Homepage des Interessensverband Versicherungsagenten IVVA.

Mag. Stephan Novotny und Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche

Für Rückfragen:

MAG. STEPHAN M. NOVOTNY

Rechtsanwalt-Attorney at Law / Akademischer Versicherungskaufmann / Collaborative Law Lawyer
Weihburggasse 4/2/26, A-1010 Wien
Tel: +43 / 1 / 512 93 37, Fax +43 / 1 / 512 93 37 93, Mob. +43 / 664 / 143 29 11
kanzlei@ra-novotny.at **www.ra-novotny.at**

Foto: Stephan Huger