3-Jahre Datenschutz-Grundverordnung (DSGVO)

Die dringlichsten Aufgaben zum Erledigen, die wichtigsten Urteile.

Seit 25.5.2018 gibt es keine Ausreden mehr: Mit **existenzbedrohenden Strafen** von bis zu 20 Mio. Euro oder 4 % des Konzern-Umsatzes versucht die EU auch die schwarzen Schafe an die Leine zu nehmen. Datenschutz hat nun oberste Priorität. Wir müssen also die **Sicherheit der Daten** (egal ob Kunden, Partner, Mitarbeiter, etc.) **garantieren.** Umfangreiche Vorkehrungsmaßnahmen waren und regelmäßige **Kontrollen sind nötig.**

3 Jahre nach Start: Haben Sie alles erledigt? Sind Adaptionen nötig?

Solche Jahrestage wie eben „3-Jahre-seit-Inkrafttreten" sollten **ein Anlass** sein, um sich wieder von Grund auf mit der DSGVO zu beschäftigen und **alles zu kontrollieren:**

Etwa: **Stimmen die Formulare noch** (etwa das Verfahrensverzeichnis), die man damals ausgefüllt hatte oder hat man z.B. neue Partner (z.B. eine neue Druckerei?), neue Datenanwendungen (etwa neue Software)? Verwendet man eine **Software**, die damals dank Privacy Shield-Abkommens zwischen EU und USA legal war. Aber nun nach EuGH-Urteil **nicht mehr DSGVO-konform** ist? Was muss man nun eigentlich tun?
Hat man die **korrekte Adresse der Datenschutzbehörde** (hat sich geändert!), um im Notfall eine Datenpanne binnen 72 Stunden melden zu können? Usw. usf.

Wir nehmen den Jahrestag zum Anlass, um Sie auf die **wichtigsten Punkte** der DSGVO und auf die **wichtigsten Urteile und Strafen** hinzuweisen.

Warum soll man das alles einhalten? Neu: Auch Schadenersatzforderungen drohen!

In Deutschland gibt es erste Urteile und eine Entscheidung des Verfassungsgerichts, die künftig viel öfters Schadenersatz-Zahlungen in beachtlicher Höhe wahrscheinlich machen.
Alle Details zu diesem Urteil können Sie hier nachlesen…

Das „Kleine 1x1 des Datenschutzes"

Auch 3 Jahre nach Wirksamwerden der DSGVO ist **noch vieles unklar,** noch nicht ausjudiziert. Was auch daran liegt, dass große Datenkraken gegen erste Strafen in Berufung gingen und noch keine Urteil dazu vorliegen.

Aber es gibt **einige Punkte, die unbedingt erfüllt sein sollten.** Der deutsche Datenschutz-Experte Sebastian Kraska sprach im Computer-Magazin com! professionell unlängst vom „Kleinen 1x1 des Datenschutzes". Und weiter: „Unternehmen können **nicht auf das Verständnis der Aufsichtsbehörden hoffen, wenn sie nicht zumindest** diese Basisthemen abdecken", so Kraska. Zum **Nachlesen** hier klicken…

Wir haben uns von diesem „1x1" inspirieren lassen, seine Auflistung der „wichtigsten Punkte" **für Österreich adaptiert und um eigene Punkte ergänzt.** Aber eine Garantie, dass damit die DSGVO in jedem Fall korrekt erfüllt ist, wenn das abgehakt wurde, gibt es natürlich nicht. Aber ein guter Start wäre es allemal…

Folgende Punkte sollten Unternehmen laut Kraska und Mag. Novotny **auf jeden Fall sofort umsetzen,** wenn sie es nicht schon längst getan haben. Die meisten Punkte haben wir in den letzten Monaten **im BAV-Newsletter bereits sehr detailliert behandelt.** Die entsprechenden Links finden Sie beigefügt!

Zum „kleinen 1x1 des Datenschutzes" kommen Sie hier…

Auswahl einiger wichtiger Urteile, zum Besser werden!

Die diversen Datenschutzbehörden trafen Entscheidungen, die auch für uns in Österreich relevant und zu befolgen sind, weil die **DSGVO eine Europäische Verordnung ist, die europaweit gleich anzuwenden** ist. Hier zum Erinnern eine kurze Auswahl von Entscheidungen, über die wir in den BAV-Newslettern bereits berichtet haben.

+) **50-Millionen**-Euro-DSGVO-Strafe gegen Google bestätigt
Google kam sogar noch mit einem blauen Auge davon, denn die Höchststrafen können laut DSGVO bis zu EUR 20 Mio. pro Unternehmen oder sogar 4% des Umsatzes bei Konzernen betragen (bei Google hätte das also weit mehr als EUR 50 Mio. ausmachen können!).

+) **9,55 Mio. wegen telefonischer Auskunft an Unberechtigte, mangelnde TOMs**
Beim deutschen Telekommunikationsunternehmen „1&1" war es offensichtlich üblich, dass man Anrufern, wenn sie Namen und Geburtsdatum eines Kunden nennen konnten, Auskünfte erteilte, die „weitreichende Informationen zu weiteren personenbezogenen Kundendaten" enthalten konnten. Erstaunlich ist, dass so eine Mega-Strafe verhängt wurde, **trotzdem** die Behörde anerkannte, dass das Unternehmen im Verfahren **kooperativ** gewesen sei. Aber: „Das Unternehmen hatte keine hinreichenden technisch-organisatorischen Maßnahmen (also TOMs) ergriffen, um zu verhindern, dass Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können."

+) 400.000 wegen Verfehlungen bei den TOMs
Ein portugiesisches Krankenhaus wurde zu dieser „geringen" Strafe verurteilt, weil man sich kooperativ gegenüber der Behörde zeigte und aktiv an der Behebung der Mängel mitgearbeitet hatte. Die **Verfehlungen betrafen die TOMs,** also die technischen und organisatorischen Maßnahmen, die im Zuge der DSGVO-Umsetzung realisiert werden mussten. Konkret wurden beim Ausscheiden von Mitarbeitern **nicht sofort deren Zugriffsmöglichkeiten deaktiviert.**

+) Verheimlichtes Datenleck wird teuer
Der Essenslieferant Foodora (gehört in Österreich zu Mjam) **meldete nicht, dass man gehackt** wurde. Als Jahre später die Daten von 727.000 Kunden im Internet zum Kauf angeboten wurden, drohen nun der Mutter eine Strafe von 4% des weltweiten jährlichen Umsatzes. Daher bei Daten-„Unfällen" und Hacker-Angriffen sofort prüfen, ob eine Meldung nötig ist und dies binnen 72 Stunden (egal ob Wochenende oder Feiertag) der Datenschutzbehörde melden.

+) **25.000-Euro**-Strafe, **weil Datenschutzbeauftragter fehlte**
Ein spanischer Lieferdienst wurde – nach der Beschwerde zweier Betroffener – verurteilt. Aufgrund der

zahlreichen und umfangreichen Datenverarbeitungen hätte man einen Datenschutzbeauftragten bestellen müssen, hat dies aber nicht getan.

+) **EUR 5.000**, **weil kein Auftragsverarbeiter-Vertrag** (AVV) mit Dienstleister bestand
Daher: Prüfen Sie, ob Sie von allen Ihren Dienstleistern einen AVV haben.

+) **EUR 5.000 Schadenersatz** wegen **verspäteter Auskunftserteilung**
Das Arbeitsgerichts Düsseldorf sprach einem ehemaligen Angestellten wegen einer zu späten und unvollständigen Auskunftsbeantwortung zu. Grund: Verletzung der Auskunftspflicht.

+) **Datenpanne beim E-Mail-Versand:** Zu viele Mail-Adressen unter AN: statt BCC:
E-Mail-Adressen sind personenbezogene Daten und dürfen daher Dritten – wie in der betroffenen Massenaussendung – nicht offen zugängig gemacht werden.
Und 2. Tipp: Passen Sie auch bei der automatischen Namensergänzung von Outlook auf, dass aus den Anfangsbuchstaben eines Namens nicht ein falscher Name aus Ihren Kontakten gewählt und das Mail an einen unbeteiligten Dritten gesendet wird. Beides ist eine Datenpanne.

Mehr Details zu den skizzierten Urteilen finden Sie hier … und hier… und hier…

PS: Im nächsten BAV-Newsletter sehen wir uns an, was genau man **unter den TOMs versteht** und worin die Unterschiede zwischen **Zutritts-, Zugangs- und Zugriffskontrolle** bestehen und bringen typische Umsetzungs-Beispiele dafür.
Auch die korrekte **Vorgehensweise bei Datenpannen** sehen wir uns im Detail an.

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