Teil 2: Rückschau auf aktuelle Urteile zur DSGVO.

Was lernen wir aus den betroffenen Verfahren? Praxistipps zum Besserwerden.

Im ersten Teil (hier klicken **zum Nachlesen**) haben wir berichtet, dass die Datenschutzbehörde sehr aktiv nach weiteren Mitarbeitern sucht. Und per Newsletter verkündet hat, dass das – von der Politik kommunizierte – **Prinzip „Verwarnen statt Strafen" nicht eingehalten** werde.

Daher sehen wir uns diverse Urteile zum Thema DSGVO näher an. Was wurde bestraft? Mit welcher Höhe? Und wie sollte man es besser machen? Im ersten Teil spannte sich die **Strafhöhe von einigen Tausend bis hin zu 50 Mio. Euro**. Zum Nachlesen hier klicken …

Heute sehen wir uns weitere Urteile näher an. Bitte checken Sie, ob das auf Ihr Unternehmen eventuell auch zutreffen könnte und falls ja, bitte ändern.

a) Datenpanne beim E-Mail-Versand

Beginnen wir mit einem Fall, der wirklich **jedem passieren kann.** Zwar gibt es noch kein Urteil dazu, das „Hoppala" ist aber laut DSGVO eine **Datenpanne** und kann daher bestraft werden.

Wie Sie vor einiger Zeit den Medien entnehmen konnten – u.a. DER STANDARD, Oe24 – nahm eine Corona-Infizierte an einer Party in Graz teil. Daraufhin wollten die **Gesundheitsbehörden alle Gäste rasch informieren.** Damit sie sich sofort in Quarantäne begeben und auf Covid-19 testen lassen sollen. Und prompt passierte hier die Panne. Die E-Mail-Adressen von allen 222 „Verdachtsfällen" waren im E-Mail offen ersichtlich. Sie waren unter „**An" anstelle unter „Bcc"** in das E-Mail eingegeben worden. Die Leiterin des Grazer Gesundheitsamtes hatte sich sofort für diesen Fehler entschuldigt und auch eine Meldung an die Datenschutzbehörde wurde gemacht, denn es handelt sich hierbei um eine **Datenschutzverletzung.**

Warum? Die **E-Mail-Adressen sind personenbezogene Daten** und dürfen daher Dritten – wie hier in dieser Massenaussendung – nicht offen zugängig gemacht werden. Es kommt erschwerend dazu, dass es sich hier beim Inhalt des E-Mails um einen **medizinischen Zusammenhang** handelt, hier also besondere Vorsicht geboten ist. Womöglich könnten Betroffene sogar Schadenersatz verlangen.

Tipp: Niemals mehrere oder sogar viele E-Mail-Adressen von **unbeteiligten Dritten öffentlich einsehbar versenden.**

Und noch eine tägliche Gefahr:
Gerade bei Smartphones oder PCs kann die automatische Namensergänzung zu Fehlern führen. Wenn also die **Autokorrektur** aus den Anfangsbuchstaben eines Namens einen **falschen Namen aus Ihren Kontakten wählt** und das Mail an einen unbeteiligten Dritten sendet, dann ist auch das eine **Datenpanne.**
Tipp: Prüfen Sie vor dem Absenden eines E-Mails immer die E-Mail-Adressaten, ob wirklich die gewünschten Namen aufscheinen. Andernfalls verletzen Sie eines der Betroffenenrechte, nämlich jenes hinsichtlich der Geheimhaltung.

Und wie wäre das ordnungsgemäße Vorgehen bei Datenpannen?
Innerhalb von **72 Stunden** ist die Datenschutzbehörde umfassend zu informieren, wenn ein **Risiko für die**

Gesundheit, den Ruf oder das „Vermögen" der betroffenen Personen besteht. Wird eine solche Meldung gar nicht oder zu spät eingeleitet, muss ein Unternehmen mit **hohen Strafen** rechnen! Das ist ein derart wichtiges Thema und die Abschätzung, wann man nun genau die Behörde informieren muss, keine leichte. Daher werden wir uns das in einem der nächsten BAV-Newsletter näher ansehen.

b) Datenleck bei Foodora wird teuer

Persönliche Daten von 727.000 Kunden des Essenslieferdienstes Foodora wurden in 14 Ländern bereits 2016 gestohlen. Etwa Namen, Adressen, Telefonnummern, Passwörter. Das berichteten mehrere Medien, wie etwa die Süddeutsche Zeitung. Diese Daten wurden laut Medien in einem Online-Forum präsentiert. Erst dadurch wurde die Datenpanne der Öffentlichkeit bekannt.

Daraufhin bestätigte Delivery Hero, das Mutterunternehmen von Foodora, in einer offiziellen Stellungnahme den Vorfall. Konkret sollen in Österreich rund 24.000 Kunden betroffen sein. In Österreich gehört Foodora nun zu Mjam.

Für diese Datenpanne, die noch dazu wahrscheinlich nicht binnen 72 Stunden gemeldet wurde, droht nun eine **Strafzahlung in der Höhe von bis zu 4 Prozent** des weltweiten jährlichen Umsatzes von Delivery Hero.

Tipp: Um zu **überprüfen, ob Ihre Daten gehackt** worden sein könnten, gibt es eine einfache Möglichkeit, die auch von Datenschützern empfohlen wird: https://haveibeenpwned.com/

Das ist eine Seite, die alle Daten von öffentlich bekannt gegebenen Hackerangriffen sammelt. **Tippen Sie dort Ihre E-Mail-Adresse oder Telefonnummer ein,** dann erhalten Sie an diese E-Mail-Adresse alle Infos gesandt, die man dazu gefunden hat. **Das Ergebnis** schaut dann in etwa so aus:

Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
adobe.com	Okt. 2013	✓	152.375.851	Betroffen	–	–	–	–	–	–	–	–

Obige Grafik bedeutet, dass meine eigene – alte – E-Mail-Adresse bei einem Hack gegen Adobe betroffen war. Und auch mein – altes – **Passwort gestohlen** worden war (daher rot unterlegt). Alle anderen Felder sind grün unterlegt, also wurden nicht gestohlen.

Tipp: Wenn Ihre E-Mail-Adresse gehackt wurde, überlegen Sie, wo Sie diese Mail-Adresse noch als Benutzername im Einsatz (z.B. bei Amazon usw.) haben und überlegen Sie weiter, mit welchen Passwörtern Sie diese E-Mail-Adresse genutzt haben. Dann **sofort das Passwort überall ändern!**

b) EUR 11.000 Strafe nach Datenleck bei Gesundheitsdaten

Im Newsletter von meineberater.at wurde von einem Fall berichtet, bei dem Gesundheitsdaten aufgrund menschlichen Versagens unbeabsichtigt Unbefugten zugänglich gemacht wurden.
Die Datenschutzbehörde verhängte eine DSGVO-Strafe in der Höhe von EUR 11.000.

Der Anlassfall betraf zwar eine Klinik, dennoch sollte auch **unsere Branche dieses Urteil als Warnschuss ansehen,** haben doch auch wir immer wieder mit Gesundheitsdaten zu tun, die als sensible Daten nach der

DSGVO gelten und daher besonders geschützt werden müssen. Vermittler und Versicherer haben etwa bei Anträgen von Lebens-, Berufsunfähigkeits- und ähnlichen Versicherungen mit Gesundheitsdaten der Kunden zu tun.

Tipp: Achten Sie also besonders auf diese spezielle Datenkategorie, sichern Sie diese besonders gut, übermitteln Sie diese **nur auf gesicherten Wegen** (mit eingeschriebenem Brief, verschlüsseltem E-Mail etc.).

Die Datenschutzbehörde stellte im obigen Verfahren fest, dass **keine ausreichenden technischen und organisatorischen Maßnahmen (TOMs)** getroffen wurden, die solche unbeabsichtigten Veröffentlichungen verhindert hätten.

Tipp: Prüfen Sie regelmäßig Ihre TOMs und **schulen Sie Ihre Mitarbeiter,** damit diese ebenso DSGVO-konform arbeiten. Das Thema TOMs ist sehr umfassend. Dabei ist etwa die **Raumsituation** (Videoüberwachung, Gebäudesicherung, einbruchsichere Türen, versperrbare Räume/Schränke usw.) zu prüfen.

Auch die **Software** fällt hier hinein: Hier gehören etwa das Vergeben von sicheren Passwörtern auf PCs, besondere **Admin-Rechte bei Server-Zugriffen** und das Aufzeichnen von Zugriffen etc. dazu. Ebenso die Verschlüsselung von Dateien, die Sie via E-Mail versenden! Dazu neueste Software-Updates, Virenschutz, Firewall etc.
Weiters müssen Sie die **regelmäßige Speicherung** Ihrer Daten auf verschiedenen Medien an verschiedenen Orten und ein **Verfahren für den GAU** (größtmöglich anzunehmenden Unfall, etwa Hackerangriff) und das Wiederherstellen der Daten und das Informieren der Datenschutzbehörde und aller Betroffenen definieren und dokumentieren. Soweit ein paar Ideen, was alles unter die TOMs fällt.

Quellen und Mitarbeit: Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche (www.b2b-projekte.at), DER STANDARD, Oe24, Newsletter von meineberater.at, futurezone.at, sueddeutsche.de, golem.de

RA Mag. Stephan Novotny
Weihburggasse 4/2/26
1010 Wien

kanzlei@ra-novotny.at

www.ra-novotny.at

PS: Gerne stehe ich den Zurich-BAV-Newsletter-Lesern bei Rückfragen, Beratungen, Vertretungen unter **Hinweis „Zurich"** zum Sonderpreis zur Verfügung!