Mag. Günter Wagner
B2B Projekte
für Finanz- und Versicherungsbranche

DSGVo: Viele neue (teure) DSGVO-Strafen. Sind Sie vorbereitet? Was lernen wir aus den betroffenen Verfahren?

Im heutigen **6. DSGVO-Praxis-Beitrag** sieht sich der auf Versicherungsrecht und DSGVO spezialisierte Jurist **Mag. Stephan Novotny die zahlreichen Urteile zum Datenschutz** genauer an.

Knapp vor Weihnachten oder **zwischen den Feiertagen ist es vielleicht eine gute Zeit,** um sich mit den Datenschutz-Urteilen der letzten Wochen ein wenig auseinander zu setzen. Hätten Sie alles korrekt erfüllt, was die Datenbehörden bestraft haben oder finden Sie in Ihrem Unternehmen doch noch die eine oder andere skizzierte "Problemsituation"?

RA Mag. Stephan Novotny berichtet was die Behörde kritisierte, mit welchen Strafen sie die Vergehen sanktionierte und was wir daraus lernen können, um DSGVO-fit zu agieren. Es gab **einige Millionen-Strafen,** aber auch **viele „kleine" mit einigen Tausend Euros,** die aber leicht zu verhindern gewesen wären, hätte man „Grund-Prinzipien" der DSGVO befolgt. Daher gibt Mag. Novotny auch **Tipps für die Praxis!**

Bedenken Sie: Die **Datenschutzbehörde sucht aktiv nach weiteren Mitarbeitern**, das lässt darauf schließen, dass ein „heißer Herbst" bevorsteht.

Keine Schonfrist. Kein Verwarnen nötig! Verlassen Sie sich nicht auf die **in den Medien oftmals zitierte Schonfrist** und auch nicht auf das „Verwarnen statt Strafen".
Die Datenschutzbehörde hat in ihrem eigenen Newsletter 2/20 die Frage gestellt: „Muss die Datenschutzbehörde bei erstmaligen Verstößen verwarnen statt strafen?" Und sich selbst geantwortet: „Im Ergebnis ist daher festzuhalten, dass die DSB durch den - neu eingeführten - § 11 DSB … … in ihrem Ermessen im Rahmen der Verhängung von **Sanktionen nicht beschränkt wird und daher auch bei erstmaligen Verstößen Geldbußen nach Art. 83 DSGVO verhängen kann".**

Die **bisher erschienen Praxis-Beiträge zur DSGVO von Mag. Novotny** beschäftigten sich mit folgenden Themen:

DSGVO 1: DSB-Urteil zur **maximalen Speicherdauer:** Wie Freibeweisen ohne Unterlagen? Hier weiterlesen...
DSGVO 2: **TOMs:** Was lernen wir aus **Megastrafe?** Hier weiterlesen...
DSGVO 3: **Ausweiskopien:** Nie unverändert speichern oder versenden! Hier weiterlesen...
DSGVO 4: **Millionenstrafe wegen telefonischer Auskunft!** Was lief schief? Wie besser machen? Hier weiterlesen...
DSGVO 5: Was fordert **EuGH zur Einwilling bei Cookie**-Nutzung auf **Webseite?** Abmahnungen vermeiden! Hier weiterlesen...

Alle bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen...
Den aktuellen Beitrag können Sie am als PDF anfordern. Ein Mail mit "JA zu INFO" an g.wagner@b2b-projekte.at genügt.

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

DSGVo: Viele neue (teure) DSGVO-Strafen. Sind Sie vorbereitet? Was lernen wir aus den betroffenen Verfahren?

Um Sie auf das nächste Jahr gut vorzubereiten, haben wir für Sie **Urteile der vergangenen Wochen zusammengefasst.** Darin erfahren Sie, was die Behörde kritisierte, mit welchen Strafen Sie die Vergehen sanktionierte und was wir daraus lernen können. Links zu Beiträgen, in denen wir beschreiben, wie man es besser machen sollte, sind an den jeweiligen Stellen eingebaut.

Es gab **einige Millionen-Strafen,** aber auch **viele „kleine" mit einigen Tausend Euros,** die aber leicht zu verhindern gewesen wären, hätte man „Grund-Prinzipien" der DSGVO befolgt. Vielleicht können Sie sich in den nächsten Tagen/Wochen ein wenig Zeit nehmen und **sich überlegen, ob Sie in Ihrem Unternehmen DSGVO-fit** sind oder eventuell auch die eine oder andere oben skizzierte „Problemsituation" haben. Und diese sanieren.

Wichtig: Wir zitieren immer wieder auch **Datenschutz-Urteile aus anderen Staaten der EU.** Der Grund ist einfach erklärt: Die DSGVO war keine Richtlinie, sondern eine Verordnung die seit dem 25. Mai 2018 **UNMITTELBAR in allen EU-Mitgliedstaaten** gegolten hat. D.h. die DSGVO hat die Datenschutzregeln vereinheitlicht. Somit sind auch Urteile anderer europäischer Datenschutzbehörden auch für andere Länder aussagekräftig und ein Hinweis darauf, wie die österreichische Datenschutzbehörde ein gleichartiges Vergehen beurteilen wird.

a) 50-Millionen-Euro-DSGVO-Strafe gegen Google bestätigt

Um Sie gleich an die Existenzbedrohung durch die DSGVO zu erinnern, darf ich gleich zu Beginn mitteilen, dass die Millionen-Strafe gegen Google kürzlich bestätigt wurde. Das Urteil war schon im Sommer bekannt, allerdings hatte Google Einspruch erhoben, dieser wurde aber vor wenigen Wochen zurück gewiesen. Google kommt sogar noch **mit einem blauen Auge davon,** denn die Höchststrafen können laut DSGVO bis zu 20 Mio. Euro oder sogar 4 % des Konzern-Umsatzes betragen.

b) 25.000-Euro-Strafe, weil Datenschutzbeauftragter fehlte

Im Newsletter von meineberater.at wurde von einem Fall berichtet, wo - nach der Beschwerde zweier Betroffener - die spanische Datenschutzbehörde gegen einen Lieferdienst Ermittlungen einleitete. Mit dem Ergebnis, dass das Unternehmen aufgrund **der zahlreichen und umfangreichen Datenverarbeitungen einen Datenschutzbeauftragten bestellen hätte müssen, dies aber nicht getan** hatte.
Achtung: Wird – trotz Verpflichtung – kein Datenschutzbeauftragter bestellt, droht eine Strafe von bis zu EUR 10 Mio. oder 2 % des letztjährigen weltweiten Jahresumsatzes.
Tipp: Prüfen Sie also, ob Ihr Unternehmen einen Datenschutzbeauftragten benötigt.

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

c) 5.000 Euro weil kein Auftragsverarbeiter-Vertrag mit Dienstleister bestand

Sie müssen mit Ihren Dienstleistern, also Auftragsverarbeitern einen AVV, einen Auftragsverarbeiter-Vertrag abschließen. Sinn ist, dass darin das beauftragte Unternehmen **bestätigt, dass es ebenfalls die DSGVO einhält,** also die von Ihnen übermittelten personenbezogenen Daten DSGVO-konform verarbeitet, geheim hält, etc.
MeineBerater.at zitiert ein Urteil der deutschen Datenschutzbehörde. Diese stellte bei einem Unternehmen fest, dass kein Auftragsverarbeiter-Vertrag mit einem von ihm beauftragten Dienstleister abgeschlossen wurde. Und verhängte hierfür ein Bußgeld von 5.000 Euro.
Tipp: Prüfen Sie, ob Sie **von allen Ihren Dienstleistern einen AVV** haben. Falls nicht, sofort urgieren und notfalls die Zusammenarbeit beenden. Prüfen Sie auch regelmäßig die **Einhaltung der TOMs** bei Ihrem Auftragsverarbeiter. Und die Schulung seiner Mitarbeiter.

d) 5.000 Euro Schadenersatz wegen verspäteter Auskunfts-Erteilung

Erich von Maurnböck berichtete in einem Newsletter, dass das Arbeitsgericht Düsseldorf wegen einer zu späten und unvollständigen Auskunftsbeantwortung einen **immateriellen Schaden** erkannt und in erster Instanz € 5.000 als Schadenersatz zugesprochen hat.
Ein Ex-Mitarbeiter nutzte sein Recht auf Auskunft und wollte von seinem Ex-Arbeitgeber wissen, welche Daten er von ihm gespeichert habe. Erst Monate später erhielt er eine Auskunft. Also weder **weder fristgerecht, und noch dazu unvollständig**.
Damit behinderte der Arbeitgeber die Ausübung der **Betroffenen-Rechte** nach der DSGVO und beging eine **Verletzung der Auskunftspflicht.** Das Urteil ist noch nicht rechtskräftig, hätte aber großes Gefahrenpotential, wenn es Bestand hat.
Tipp: Nehmen Sie Auskunftsbegehren ernst! Erarbeiten Sie ein Auskunfts- und Löschkonzept, damit das Begehren von einem Zuständigen korrekt und zeitgerecht bearbeitet wird (4 Wochen Frist).

e) 15.000 Euro DSGVO-Strafe wegen abfotographierter Teilnehmerliste

Erich von Maurnböck berichtete kürzlich in einem Newsletter über ein Urteil der rumänischen Behörde: In einem Hotel wurde eine **Liste von Frühstücksgästen** abfotographiert und im Internet veröffentlicht. Zwar hat das Hotel selbst diese Datenpanne vorschriftsmäßig an die Datenschutzbehörde gemeldet. Trotzdem verhängte die Behörde eine **Geldstrafe von 15.000 Euro** wegen dieser Datenschutzverletzung. Begründung: **Mangel bei den TOMs** (technischen und organisatorischen Maßnahmen) des Hotels, daher war nicht ausreichend sichergestellt, dass die Mitarbeiter die personenbezogenen Daten nur rechtmäßig verarbeiten.
Tipp: Teilnehmerlisten gibt es überall. Z.B. bei Seminaren, Messen, etc. Achten Sie darauf, dass sie **nicht in falsche Hände** kommen. Nicht im Internet auftauchen. **Schulen Sie** Ihre Mitarbeiter! Auch Studenten, die Ihnen bei einem Event helfen und vielleicht nicht so datenschutz-firm sind.

f) Taxifahrer fotografiert Führerschein und versendet ihn über WhatsApp

MeineBerater.at schildert einen besonders krassen Fall in Österreich. Da ein Fahrgast eines Taxis zu wenig Bargeld hatte, fotographierte der Fahrer **Führerschein / Bankomatkarte ab** und leitete diese via **WhatsApp** an eine dritte Person weiter.
Eine Beschwerde bei der Datenschutzbehörde war erfolgreich. Es wurde ein Verstoß gegen den Grundsatz der Datenminimierung und eine Verletzung der Geheimhaltung festgestellt. Weder die Datenerhebung, also das Abfotografieren, noch das Weiterleiten war rechtmäßig. Der Rechtfertigungsgrund „des **überwiegenden berechtigten Interesses“** des Taxiunternehmens wurde nicht akzeptiert.

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

Ob das Verfahren schon rechtskräftig abgeschlossen ist, lässt sich momentan nicht feststellen. Erschwerend bei diesem Fall ist die **Verwendung von WhatsApp,** von der wir immer wieder **dringend abraten.** Verwendet man WhatsApp, werden Daten automatisch in die USA weitergeleitet (mit Facebook geteilt, etc) – und dafür hat Ihnen sicher kein Kunde freiwillig seine Einwilligung erteilt.
Tipp: Hände weg von WhatsApp im beruflichen Umfeld. Schulen Sie Ihre Mitarbeiter!

g) Datenpanne beim E-Mail-Versand

Ein besonders "böses Hoppala" ist einer Gesundheitsbehörde in Graz passiert. Jedoch ein Hoppala, das **Jedem passieren kann.** Zwar gibt es unseres Wissens nach noch kein Urteil dazu, aber Fakt ist das „Hoppala“ ist laut DSGVO eine **Datenpanne** und kann daher bestraft werden.

Wie Sie 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:** eingegeben worden. Die Leiterin des Grazer Gesundheitsamtes hat 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. Dazu kommt erschwerend, dass es sich hier um einen **medizinischen** Zusammenhang handelt, hier ist also besondere Vorsicht geboten. Womöglich könnten Betroffene sogar Schadenersatz verlangen.
Tipp: Niemals mehrere E-Mail-Adressen von **unbeteiligten Dritten öffentlich einsehbar versenden.**

Und noch eine tägliche Gefahr:

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

h) Datenleck bei Foodora wird teuer

Persönliche Daten von 727.000 Kunden des Essenslieferdienstes Foodora wurden in 14 Ländern bereits 2016 gestohlen. Etwa Namen, Adressen, Telefon-Nummern, Passwörter. Das berichteten mehrere Medien, wie etwa die Süddeutsche Zeitung. Diese Daten wurden laut Medien am 19. Mai in einem Online-Forum präsentiert, das für gestohlene Daten bekannt sei. Dadurch erst wurde die Datenpanne der Öffentlichkeit bekannt.
Darauf 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.

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

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. Darüber haben wir bereits berichtet: **Zum Nachlesen** hier klicken...

i) 11.000 Euro Strafe nach Datenleck bei Gesundheitsdaten
Im Newsletter von meineberater.at wurde von einem Fall berichtet, wo Gesundheitsdaten aufgrund menschlichen Versagens unbeabsichtigt Unbefugten zugänglich gemacht wurden. Die Datenschutzbehörde verhängte eine DSGVO-Strafe in der Höhe von 11.000 Euro.
Der Anlassfall betraf zwar eine Klinik, dennoch sollte auch **unsere Branche dieses Urteil als Warnschuss ansehen,** haben wir doch 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 Datenkategorie, sichern Sie diese besonders gut, übermitteln Sie diese nur auf gesicherten Wegen (eingeschriebenem Brief, verschlüsselte E-Mail, etc.)
Tipp: Prüfen Sie regelmäßig Ihre TOMs und schulen Sie Ihre Mitarbeiter, damit diese ebenso DSGVO-konform arbeiten.

Quellen: Newsletter der Datenschutzbehörde und von www.meineberater.at, IVVA Homepage, Der Standard, Oe24, futurezone.at, sueddeutsche.de, golem.de

Alle bisherigen IDD und DSGVO-Praxisbeiträge können Sie **hier herunterladen...**
Den aktuellen Beitrag können Sie als PDF anfordern. Dazu einfach ein E-mail an g.wagner@b2b-projekte.at mit Betreff "Ja zu Infos".

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**

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