Praxis-Tipp RA Mag. Novotny: Konsequenzen einer verschwiegenen Datenpanne?

Auch immaterielle Schäden werden anerkannt. Teil 3 der Serie „Datenpanne".

Im vorletzten BAV-Newsletter fragten wir bei **Mag. Novotny, ob ein medial bekannt gewordener Fall eine Datenpanne sei („JA")** und erhielten von ihm eine **Reihe von „Datenpannen-Szenarien",** um ein Gefühl zu erhalten, was eine Datenpanne ist und was nicht und was dann zu tun ist. **Zum Nachlesen von Teil 1** dieses Beitrags klicken Sie hier…

Im letzten BAV-Newsletter fragten wir Mag. Novotny, wann eine Datenpanne der **Behörde zu melden ist und wann nicht.** Und klärten auch, wie man zu melden hat, wie schnell und welche Details. **Zum Nachlesen von Teil 2** dieses Beitrags klicken Sie hier…

Hier folgt nun der 3. Teil des Beitrags, den wir mit Mag. Novotny erstellt haben.

F) Strafen, wenn Datenpanne nicht gemeldet wurde

Was mich als Fach-Jurist immer wieder beschäftigt, ist, warum in (vielen) Unternehmen eine **Datenpanne einfach verschwiegen wird.** Und weder der Datenschutzbehörde DSB noch den Kunden gemeldet wird.
Ich kann dieses **„Kopf in den Sand stecken" überhaupt nicht nachvollziehen,** denn die DSB ist zumeist „verständnisvoll", wenn man eine Datenpanne korrekt und rechtzeitig meldet. Erklärt, wie das passieren konnte und aufzeigt, was man alles bereits getan hat (um seine Verpflichtungen nach der DSGVO zu erfüllen). Und was man tun wird, um so eine Datenpanne künftig möglichst zu vermeiden.

Mir erscheint das Risiko, dass eine Datenpanne nachträglich doch bekannt wird und sozusagen die Datenschutzbehörde „zwingt" zu handeln und somit zu strafen, wesentlich höher. Und daher wäre es auch **wesentlich vernünftiger und wirtschaftlich sinnvoller, Datenpannen zu melden.** Von der Strafhöhe abgesehen, die man sich durch eine korrekte Meldung ersparen könnte, ist der Imageschade für das Unternehmen viel größer. Und man muss **wohl kein Prophet sein, um vorherzusagen, dass die Datenschutzbehörde** so ein Unternehmen, dass sich ganz offensichtlich nicht um die Einhaltung der DSGVO kümmert, in den **nächsten Jahren genauer im Auge behalten wird.**

Mein Tipp zu dieser Frage: Wenn Sie nicht sicher sind, ob eine Datenpanne meldepflichtig ist oder nicht, dann **melden Sie im Zweifelsfall.**
Aus Sicht der Behörde macht es einen riesigen Unterschied, ob eine Datenpanne gemeldet wurde oder nicht. Erfährt die Behörde jedoch erst durch die Beschwerde einer betroffenen Person und das Unternehmen selbst hat nicht oder nicht rechtzeitig (72 Stunden nach Kenntnis) an die DSB gemeldet, dann werden wohl wesentlich strengere Maßstäbe an das Unternehmen angelegt und die Konsequenzen schlimmer sein. Weil das Verschweigen der Datenpanne zum Fehler, der zur Datenpanne geführt hat, noch dazu kommt.

Und bedenken Sie: Das **Verschweigen einer Datenpanne** hat Konsequenzen gegenüber Behörde, Kunden (können z.B. Schadenersatz verlangen) und allenfalls auch auf die Wettbewerbssituation. Ein **UWG-Verstoß** darf in solch einer Situation nicht vergessen werden: Wer sich einen Wettbewerbsvorteil aus einer Nichtanzeige an die Behörde verschafft, kann auch von der Konkurrenz auf Unterlassung und Schadenersatz geklagt werden. Der Wettbewerbsvorteil liegt schon in der mangelnden tatsächlichen Rufschädigung, der dem nichtmeldenden Unternehmer erspart bleibt, in Kosten und in einer massiven Zeitersparnis gegenüber jenen Unternehmern, die sich in einer derartigen Situation rechtskonform verhalten.

Wie schlimm kann es werden?

Das ist schwer zu sagen. Leider werden **nur die wenigsten Urteile der Datenschutzbehörden veröffentlicht** und noch weniger davon werden dem Markt bekannt.
Und natürlich macht es einen Unterschied, ob Sie z.B. eine Einladung zur Weihnachtsfeier an einen anderen Verteiler als beabsichtigt versenden. Oder ob Sie z.B. Gesundheitsdaten von Angestellten an die Personalabteilung weiterleiten (was die Kündigungsgefahr erhöhen könnte, wenn Krankheiten dadurch bekannt würden). Und ebenso ist die Zahl der Empfänger relevant, also ob es sich um eine Handvoll potenziell Betroffener handelt oder um Tausende, bis hin zu Millionen…

Trotz der geringen Zahl an bekannten Urteilen fand ich bei der **Recherche deren 3, die die große Bandbreite aufzeigen. Und Ihnen ein Gefühl geben soll, wie gefährlich und teuer das Verschweigen einer Datenpanne werden kann.**

Meine Datenschutz-Kollegin Mag.a Birgit von Maurnböck berichtete von einem **Urteil der polnischen Datenschutzbehörde**, die die Medizinische Universität Katowice **mit 5.498 Euro bestrafte,** weil bei einer Prüfung ein Video mitgelaufen war. Auf dieses Video konnten nicht nur die tatsächlich anwesenden Prüflinge, sondern auch die Dozenten und alle Personen, die für diese Lehrveranstaltung registriert waren, zugreifen. Obwohl die Gesamtzahl der Aufgenommenen gering war (knapp 150) und nur einige der Prüflinge identifizierbar waren, wurde diese Strafe verhängt.
Und zwar nicht wegen des Vorfalls, sondern „weil die Datenpanne nicht ordnungsgemäß und laut DSGVO-Vorschrift an die Datenschutzbehörde sowie an die Betroffenen gemeldet worden war". Einige der Prüflinge erfuhren erst durch andere Studenten von diesem Vorfall. Angesichts der geringen Zahl der Betroffenen und geringen Reichweite des Verstoßes eine ziemlich heftige Bestrafung, die wohl nur auf das Verschweigen zurückzuführen scheint.

Wenn dagegen eine **große Zahl von Betroffenen involviert** ist und keine Meldung an die Datenschutzbehörde passiert ist, dann gehen die Strafen in exorbitante Höhen:

So wurde gegen **Booking.com** von der holländischen Datenschutzbehörde eine **Strafe über 475.000 Euro verhängt** und nach dem großen Datenleck bei Facebook liegt der Fall nun bei der irischen Datenschutzbehörde.

Was war passiert?

Bei Booking.com war Medienberichten zufolge – siehe Link unten – ein „Sicherheitsvorfall", wahrscheinlich ein Hackerangriff **passiert. Ergebnis: Die persönlichen Daten von Hotelkunden gelangten in die Hände von Online**-Betrüger. Konkret soll es sich um 4.109 Personen gehandelt haben, darunter die Kreditkartendaten von 283 Kunden. Bei 97 dieser Datensätze konnten die Betrüger auch die Sicherheitsnummer der Kreditkartenbesitzer erbeuten. Um an noch mehr Kreditkartendaten – möglicherweise für den Handel im Darknet – zu kommen, hatten sich die Betrüger außerdem als Booking.com-Mitarbeiter ausgegeben und waren in telefonischen Kontakt zu den betroffenen Kunden getreten. So berichtet PC-Welt von diesem Fall.
Und wieder wurde die Strafe ausgesprochen, weil das Datenleck zu spät, konkret erst 22 Tage nach Kenntnis gemeldet worden war.

Zum Facebook-Datenleck:

Laut Medienberichten – Links finden Sie unten anbei – fanden **im April 2021** Experten der IT-Sicherheitsfirma Hudson Rock die **Daten von über 533 Millionen Facebook-Usern im Netz** – darunter Adressen, Geburtstage und sogar Telefonnummern. Facebook betonte damals zwar, dass es sich um "alte Daten" von vor 2019 handeln würde. Dagegen wird aber argumentiert, dass viele ihre E-Mail-Adressen und Telefonnummern in der Regel nicht ändern und sich einmal verbreitete Daten praktisch nicht aus dem Netz löschen lassen. Somit bleiben die Folgen einer Datenpanne erhalten. Daher liegt der Fall nun bei der Datenschutzbehörde. Und sollte sie ein strafbares Verhalten erkennen, dann wird das wohl **die nächste Millionenstrafe an einen Datenkraken**, schon allein aufgrund der riesigen Zahl der Betroffenen.

Dazu kommt: Datenschutz-Aktivisten und z.B. die irische Bürgerrechtsgruppe Digital Rights Ireland (DRI) fordern dazu auf, dass man als Betroffener eine Entschädigung von Facebook fordern solle. Bis zu 1.000 Euro solle man fordern.

Und das ist der nächste Bereich, der Datenpannen so teuer machen kann: Betroffene fordern Schadenersatz! Auch für „immateriellen Schaden"!

Bisher galt der „Grundsatz", dass man als Betroffener nur Schadenersatz fordern könne, wenn man einen Schaden nachweisen kann.
Die Kanzlei SBS Legal zitiert auf ihrer Webseite – link unten anbei – einen Datenpannen-Fall, der auch zu einem Schadenersatz-Urteil geführt hat, weil dem Betroffenen ein immaterieller Schaden entstanden sei. Zwar wurden statt der geforderten 2.500 Euro nur 1.000 Euro zugesprochen. **Aber für das Versenden einer einzigen Mail an einen einzigen – jedoch falschen – Empfänger ein heftiges Urteil.** Noch dazu womöglich mit **richtungsweisendem Charakter,** weil eben vom materiellen Schaden abgegangen und immaterieller Schaden anerkannt wurde.

Was war in diesem Fall passiert?

Eine Bankmitarbeiterin hatte auf dem Portal XING eine Antwort an einen Bewerber für eine Stelle in der Bank verfasst:
Inhalt in etwa: Unser Personalchef findet Ihr Profil sehr interessant. Ihre Gehaltsvorstellungen können wir nicht erfüllen. Wir können 80.000 plus variable Vergütung anbieten. Wäre das für Sie weiterhin interessant?
Diese **Antwort ging aber nicht an den Bewerber, sondern an einen unbeteiligten Dritten**. So erhielt dieser unbeteiligte Dritte persönliche und berufliche Informationen zu der Person. Diese irrtümlich versandte Mail ist ja bereits an sich ein DSGVO-Verstoß. Aber die Bank ließ weiterhin Problembewusstsein vermissen.
Denn der fälschliche Empfänger hat die Bank darauf aufmerksam gemacht, dass er diese Mail irrtümlich erhalten hatte. Trotzdem die Bank also auf ihren Fehler hingewiesen wurde, hat sie den **eigentlichen Empfänger (den Bewerber) nicht über den Fehler informiert**.
Dummerweise kannten sich der Bewerber und der fälschliche Empfänger, wodurch der Fall dem Bewerber, der zwischenzeitlich eine Absage für die Bewerbung erhalten hatte, vom Vorfall erfuhr.
Und aufgrund dieses **DSGVO-Verstoßes immateriellen Schadenersatz in Höhe von 2.500 Euro** verlangte. Das Urteil des **LG Darmstadt** vom 26.5.2020 können Sie im Wortlaut hier nachlesen:
https://openjur.de/u/2305452.html
Das Urteil wurde auch von der nächsten Instanz, dem OLG Frankfurt bestätigt und wurde heuer vom Bundesverfassungsgericht Deutschland dem EuGH, also dem Europäischen Gerichtshof, zu finalen Klärung vorgelegt.

Aber an der Auflistung der obigen 3 Fälle können Sie bereits erkennen, dass Datenpannen heikel und teuer werden können. Und noch schlimmer werden die Konsequenzen, wenn sie die Datenpanne gegenüber Datenschutzbehörde und Betroffenen verschweigen.

Daher: Datenpannen müssen **innerhalb von 72 Stunden nach internem Bemerken** des Datenschutzvorfalles der Behörde gemeldet werden. Und zwar dann, 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!

Quellen: Datenschutz-Behörde, IVVA Webseite, Newsletter Meineberater.at, Kurier, Computerbild
Weiterlese-Links
https://koehrer.de/datenpanne-meldung-strafen-und-beispiele/
https://www.computerbild.de/artikel/cb-News-Internet-Datenleck-bei-Facebook-Hier-fordern-Sie-Entschaedigung-33105085.html
https://www.computerbild.de/artikel/cb-News-Sicherheit-Daten-hunderter-Millionen-Facebook-Nutzer-erneut-im-Netz-entdeckt-30006081.html https://www.pcwelt.de/article/1194458/datenschutz-booking-com-muss-475-000-euro-strafe-zahlen.html
https://www.it-recht-kanzlei.de/lg-darmstadt-dsgvo-schadensersatz-abstrakte-schadenseignung.html
https://openjur.de/u/2391126.html
https://medien-internet-und-recht.de/volltext.php?mir_dok_id=3307
https://kurier.at/politik/inland/spoe-strategiepapier-sora-babler-finanzminister-gerhard-zeiler/402608909
https://kurier.at/politik/inland/spoe-leak-orf-sora-institut/402609512
https://ivva.at/grosse-gefahr-datenschutzpanne-wegen-vieler-empfaenger-unter-an-oder-cc-anstelle-bcc-nl-33-20/
https://datenschutzbeauftragter-dsgvo.com/dsgvo-meldepflicht-vorgehen-2/

Beste Grüße von RA Mag. Stephan Novotny und Mag. Günter Wagner, B2B-Projekte

Sollten Sie noch keinen Anwalt haben: **Mag. Stephan Novotny,** ein **auf Versicherungs- und Datenschutzrecht spezialisierter Fachanwalt** steht gerne zur Verfügung.
Für Zurich-Newsletter-Leser sogar zum **Spezialpreis.**

RA Mag. Stephan Novotny, Foto: Stephan Huger

RA Mag. Stephan Novotny
1010 Wien, Landesgerichtsstraße 16/12
kanzlei@ra-novotny.at
https://www.ra-novotny.at