Wann ist eine Datenpanne zu melden?
Hohe Strafen drohen!

Vor ein paar Wochen war es in den Medien zu lesen, dass ein bekanntes Umfrage-Institut ein „Strategie-Papier“ nicht nur an die beabsichtigen Empfänger, sondern irrtümlich an 800 Personen aus einem „Public-Health-Verteiler“ sandte. Dieses Hoppala hatte für das Institut sofort wirtschaftliche Folgen, weil der ORF eine weitere Zusammenarbeit rund um die Wahlberichterstattung (Wahlforschung, Hochrechnungen, Analysen) mit sofortiger Wirkung beendete.

Achtung: Ein Mail - an den Falschen - ist rasch versandt!
Um Ihr Problembewusstsein zu erhöhen: Es drohen hohe Strafen, wenn eine Datenpanne passiert und Sie nicht gemeldet haben, obwohl die Pflicht dazu bestanden hätte!

Obiges Hoppala wollen wir zum **Anlass** nehmen, um Sie wieder an **Datenpannen, deren Folgen und dem korrekten Verhalten laut DSGVO erinnern.** Denn wahrscheinlich ist es **jedem schon passiert:** Durch die automatische Funktion in Outlook – man tippt die ersten Buchstaben der Mail-Adresse ein und Outlook nimmt „die wahrscheinlichste“ Adresse, man schaut nicht ganz genau und drückt senden – landet die Mail schon im falschen Postkasten.

Und neben diesem wohl häufig passierenden Fall – ein mail geht irrtümlich an den falschen Empfänger hinaus – wollen wir uns auch noch **2 Fälle näher ansehen,** die wohl auch **häufiger vorkommen**, als es laut Gesetzgeber sein sollte:

- Ein Mail an offen sichtbare Mail-Adressen via cc: anstelle bcc:
- Folgen einer Datenpanne, ausgelöst durch falsche Bekanntgaben vom Kunden.

Somit **beantworten** wir heute mit **RA Mag. Stephan Novotny Fragen wie:**

- **Wann liegt eine Datenpanne vor?** Reicht schon eines der oben skizzierten **E-mails?**
- Muss es sich um **wichtigen Inhalt/Anhang handeln, um aktiv werden zu müssen?**
- Muss ich immer die **Behörde informieren?** Wenn Ja, wie schnell? Wie wäge ich ab?
- **Was tun** bei einer Datenpanne?
- **Wie Datenpanne melden? Telefonat? E-Mail? Oder? WAS** genau ist **zu melden?**
- Wie hoch hat die Behörde schon bestraft?
- Wann muss ich die **Betroffenen informieren?**
- Haben Sie einen **„Prozess“**, damit diese Tätigkeiten **rasch und richtig erfolgen?**
- Folgen einer **Datenpanne,** ausgelöst durch falsche Bekanntgabe **vom Kunden**.

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

Mag. Günter Wagner
B2B Projekte
für Finanz- und Versicherungsbranche

Die **bisher erschienen Praxis-Beiträge von Mag. Novotny auszugsweise:**

DSGVO 14: Urteil droht **250.000 €** wegen **Google Fonts** an. Hier…
DSGVO 13: Unzählige **Windows-User** bekommen **keine Updates** mehr. DSGVO-Problem! Hier…
DSGVO 12: BSI **warnt vor Kaspersky.** Was Sie wegen DSGVO tun sollten. Hier…

IDD 14: **Aufbewahrung Beratungs- und Verkaufsunterlagen:** Was sagen IDD / DSGVO dazu? Hier...
IDD 13: IDD **Aufsicht: Grobe Mängel aufgedeckt.** Welche Behörde kontrolliert bei Ihnen was? Hier...
IDD 12: Die neue Whistleblower-Richtlinie. Was müssen Sie tun? Hier...
IDD 11: Die **Behörde kommt.** Wie darauf **vorbereiten?** Hier...
IDD 10: Wann und wie darf man **Kunden und Interessenten noch kontaktieren?** TKG? Hier...

Praxis 2: Aktuelle **EDV-Gefahren**, typische **Einfallstore** und Betrugsmaschen. Hier…
Praxis 1: Praxis von **Abmahnanwälten** kann teuer werden. Hier…

ALLE bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen…
Oder kostenlos mit "JA zu INFO" an g.wagner@b2b-projekte.at anfordern.

Hier folgt nun der Beitrag, den wir mit RA Mag. Stephan Novotny erarbeitet haben.

Wann ist eine Datenpanne zu melden?
Juristische und finanzielle Konsequenzen? Hohe Strafen drohen!

A) Beispiele für konkrete „Mail-Datenpannen"-Szenarien:
a) Mail geht ungewollt an den / die falschen Teilnehmer hinaus
b) Mail geht an falsche Teilnehmer hinaus, die sich noch dazu via an: bzw. cc: sehen

Grundsätzlich handelt es sich hier **in jedem Fall um eine Datenpanne,** die näher angesehen werden muss, um zu entscheiden, **ob eine Meldung bei der Datenschutzbehörde durchzuführen ist.**

Um uns ins Thema einzustimmen und ein **Gefühl für die Praxis zu bekommen**, hier ein paar Annahmen und Überlegungen. Die detaillierten Rechtsüberlegungen folgen unten anbei.

Nehmen wir an, dass bei Fall a) ein Mail mit **keinem „relevanten Inhalt"** versandt wurde. Also ein Mail mit – sagen wir mal – „Urlaubsgrüßen" ging an Günter Wagner. Aber nicht an den Günter Wagner, der bei Firma A arbeitet, sondern bei Firma B (also nur die E-Mail-Adressen im Outlook falsch gewählt wurden). Also liegt eine Datenpanne vor, aber keine meldepflichtige (Details unten anbei). In diesem Fall bitten Sie den falschen Empfänger die Mail sofort zu löschen.

Hat man aber in dem Mail **„relevanten Inhalt" an den falschen Empfänger versandt,** dann wird es ernst. Vielleicht war eine Kundendatei dabei? Oder der Mail-Inhalt hat personenbezogene Daten oder sogar sensible Daten enthalten („hier Ihre Aids-Test-Auswertung") oder oder oder.

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

Ergebnis: Datenpanne, Meldepflicht bei Behörde, Information an die Betroffenen. Warum? (Details unten).
Und auch im Fall, dass man ein **Mail an VIELE Empfänger „offen" versendet**, liegt eine „ernste Datenpanne" vor, weil alle Empfänger die E-Mail-Adressen der anderen sehen können. Und das sind personenbezogene Daten, die man damit veröffentlicht hat.
Einschätzung: Datenpanne, Meldepflicht an Behörde, Information an die Betroffenen.
Und zwar unabhängig vom Inhalt der E-Mail. Das Versenden an An: bzw. cc: reicht aus.

Wir erinnern uns: Hierzu gab es während Corona eine **„staatliche Datenpanne",** als ein Grazer Club – wo eine Corona-infizierte Person an einer Party teilnahm – seine Gäste vor einer möglichen Ansteckung warnen wollte. Also schrieb damals das **Gesundheitsamt alle Teilnehmer per E-Mail an.** Man möge sich in Quarantäne begeben und einen Corona-Test machen. Weil man wahrscheinlich rasch sein wollte, kopierte man aber irrtümlich die E-Mail-Adressen für alle sichtbar unter AN: anstelle unter BCC:

Oft gestellte Frage: WANN liegt eine DATENPANNE vor?

War der Inhalt im geschilderten Fall eins („Urlaubswünsche") belanglos, ist der Inhalt im zweiten Fall sehr bedenklich (egal ob Aids-Test oder Kunden-Datei).
Im Falle der oben beschriebenen „staatlichen Datenpanne" treffen **2 Gründe für eine schwere Datenpanne** zu: Einerseits teilte man hunderten Personen öffentlich sichtbar mit, dass der Verdacht einer Corona-Erkrankung bestehe. Also geht es hier um **Gesundheitsdaten** und diese zählen zu den **sensiblen**, d.h. besonders schützenswerten personenbezogenen Daten. Und man verteilte – ohne Zustimmung – die E-mai-Adressen (auch personenbezogene Daten) an hunderte andere Personen.

B) Häufige Frage: WAS TUN bei einer Datenpanne?

So klar es ist, dass **in allen oben zitierten Fällen** jeweils eine **Datenpanne vorliegt,** so schwierig ist die Beantwortung und Einschätzung, in welchem Falle man was tun muss.
Konkret geht es um die Frage:
– muss man die **Datenschutzbehörde davon informieren?**
– muss man die betroffenen Personen von der Panne informieren oder nicht?

Damokles-Schwert: Gibt man KEINE Meldung ab und diese **wäre aber nötig** gewesen und ein Betroffener beschwert sich nachträglich, dann **kann das teuer** werden, denn die Betroffenen können **Schadenersatz** Weiters droht, dass die **Datenschutzbehörde** das Unternehmen ganz besonders **genau prüfen** wird. Und ebenso droht ein **Image-Verlust oder sogar Shit-Storm,** den dieses Unternehmen erleiden würde, weil man ganz offensichtlich nicht auf Kundendaten aufgepasst hat, wie es das Gesetz vorschreibt.
Eingebürgert hat sich die Praxis, dass nach einer Datenpanne, die sich auf das Versenden von E-mails mit personenbezogenen Daten Dritter bezieht, eine **E-Mail an Einzelpersonen nachgesendet** wird, in der man um das Löschung der ursprünglichen E-Mail ersucht. Allenfalls wird auch um eine Bestätigung der Löschung ersucht. Das ist als Erst-Maßnahme sicher empfehlenswert, aber die gesetzlichen Regelungen zum Datenschutz kann diese Praxis nicht aushebeln.

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) Wann Meldung an Datenschutzbehörde, wann nicht?

Hier kann ich Ihnen als Jurist nicht mit einer 100 % Sicherheit antworten, denn das kommt immer auf den Einzelfall an. **Konkret muss man sich genau ansehen, was passiert ist und welche Folgen** das für die **betroffenen Personen haben kann.**

Zentrale Frage: Kann durch die Panne ein Risiko für Gesundheit, Ruf oder Vermögen der betroffenen Person(en) bestehen?
Hier ein paar **Extrem-Beispiele**, die zeigen sollen, was ich meine:

Durch ein offen versandtes E-Mail wurde einer großen Zahl von Empfängern bekannt, dass man **Corona oder Aids oder eine sonstige geächtete Krankheit** habe. Ich nehme an, Sie können sich vorstellen, dass das die Betroffenen nicht haben wollen, weil das **negative Folgen für sie haben könnte (etwa Job-Verlust).**

Ebenso würde niemand wollen, dass seine Adresse, seine **Kontodaten, Steuergeheimnisse,** usw. im Internet kursieren. Ein weiteres klares Beispiel ist, wenn ein unverschlüsselter USB-Stick mit allen möglichen **Firmendaten verloren ging**.
Auch das Veröffentlichen von **Zahlungsschwierigkeiten** („Sie haben auf alle unsere Mahnungen nicht reagiert, wir reichen nun einen Konkurs-Antrag ein“) könnte Rufschädigung sein. Das sind wohl Fälle, wo jeder sagt, ja das ist eine schwere Datenpanne, die wir der Datenschutzbehörde melden müssen.

Es gibt aber viele andere Fälle, wo die negativen Folgen der Datenpanne für die Betroffenen wohl nicht existent oder ganz gering sind. Aber hier kann man auch einem Fehlurteil aufsitzen. Daher mein Tipp: **Bei der Abschätzung, welche Konsequenzen eine Datenpanne hat** und was man nun tun solle, sollte man auf jeden Fall den Datenschutzverantwortlichen des Hauses oder **juristischen Rat einholen.**

Wenn Sie unsicher sind: Wahrscheinlich fährt man gut mit der Strategie: **Besser zu oft melden, als gar nicht melden.** Wie gesagt, wenn Sie nachträglich von einem Betroffenen bei der Datenschutzbehörde angezeigt werden, kann es für Sie ungemütlich werden und mit Milde der Behörde ist wohl auch nicht mehr zu rechnen.

TIPP: Wenn Sie nicht melden müssen, legen Sie trotzdem einen firmeninternen **Aktenvermerk** an, beschreiben Sie darin, was genau passiert ist (etwa: E-Mail ging an 222 Empfänger öffentlich sichtbar, aber ohne „gefährlichen Inhalt“ hinaus) und was Sie getan haben, dass dies möglichst nicht mehr passieren sollte (Schulung des Verursachers oder der ganzen Abteilung, plus internem Mail mit anonymer Schilderung des Falles an den gesamten Firmen-Verteiler, um das Problembewusstsein im ganzen Unternehmen zu steigern, etc.).

D) WIE SCHNELL melden?

Wenn Sie eine Meldung an die Datenschutzbehörde abgeben müssen, beachten Sie, dass Sie **dies binnen 72 Stunden tun müssen.** Egal, ob da ein Wochenende dazwischen liegt oder der Datenschutzverantwortliche auf Urlaub und der Anwalt nicht erreichbar ist.
Auch da beschreiben Sie, was passiert ist und welche Maßnahmen Sie bereits gesetzt haben.

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

HOHE STRAFEN bei Nichtmelden!
Meine Kollegin Mag.a Birgit von Maurnböck hat in einem Newsletter ein Urteil der polnischen Datenschutzbehörde zitiert, die **5.498 Euro** verhängte. Nicht weil die Datenpanne passiert sei, sondern weil „die Datenpanne nicht ordnungsgemäß und laut DSGVO-Vorschrift an die Datenschutzbehörde sowie an die Betroffenen gemeldet worden war“.

E) Wie melden Sie die Datenpanne? Telefonat? E-Mail? Oder?

Über den Link „www.dsb.gv.at“ kommen Sie zur Website der österreichischen Datenschutzbehörde.
Über den Menü-Punkt „Download“ kommen Sie zu einem Formular, das für die Meldung von Datenpannen vorgesehen ist.

Einfach runterscrollen bis zum Punkt „Meldungen von Verletzungen des Schutzes personenbezogener Daten“. Das Formular ist von Ihrem Datenschutzbeauftragten / Datenschutzkoordinator / Rechtsanwalt auszufüllen und innerhalb von 72 Stunden abzuschicken. Kein Wochenende, kein Urlaub verlängert diese Frist.

Was genau ist zu melden?
Das Formular fragt zunächst die Kontaktdaten von Verantwortlichen / Datenschutzbeauftragten ab.
Dann müssen Sie die Datenschutzverletzung beschreiben, die Kategorien der betroffenen Personen angeben (etwa Kunden, Mitarbeiter, Patienten, Kinder), die ungefähre Anzahl der betroffenen Personen sowie welche Art von Daten verloren ging (Gesundheits-, Bankdaten, politische Meinung…). Wann ist der Vorfall („Verletzung“) passiert und wann wurde er bekannt? Sowie Beschreibung der wahrscheinlichen Folgen der Panne („Bloßstellung, Diskriminierung, finanzieller Verlust, Haftung gegenüber Kunden, Identitätsdiebstahl“)
Dann müssen Sie beschreiben, was Sie getan haben „zur Behebung der Verletzung des Schutzes“ und zur „Abmilderung der möglichen Auswirkungen“.

Tipp: Prozess einführen: Vorsicht ist besser als Nachsicht
Wenn Sie sich durchlesen, was Sie alles der Behörde binnen 72 Stunden melden müssen – womöglich noch über das Wochenende und während eines Hacker-Angriffs – dann scheint klar zu sein, dass man nicht erst dann mit Krisen-Management beginnen kann.
Sondern es muss schon vorher ein **Krisenplan** bestehen, der angibt, wer wie die Datenpanne firmenintern wem meldet und was dann passieren muss.
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

Also: **Klare Regelung des Vorgehens** bei Datenpannen! Keinesfalls sollte derjenige, der die Panne entdeckt, sofort die Behörde kontaktieren.
Sondern zuerst firmenintern zum Datenschutzverantwortlichen bzw. Geschäftsführung gehen.
Die für Datenschutz verantwortlichen Personen sollten eine **Checkliste**, z.B. mit allen wichtigen Kontaktpersonen (Rechtsabteilung, externe Juristen, EDV-Experten, etc.) haben. Auch die Kontaktdaten einer Cyber-Versicherung können hilfreich sein, wenn die Datenpanne mit einem Hackerangriff einhergeht.

Wichtig ist natürlich auch, dass das **Verarbeitungsverzeichnis** korrekt ausgefüllt wurde und aktuell ist. Nur so können Sie binnen weniger Stunden bekannt geben, welche Datenkategorien von der Datenpanne betroffen sind und dies im Formular der Datenschutzbehörde bekannt geben.
Und wenn alle Informationen grob gesichtet wurden, sollten Geschäftsführung und alle für den Datenschutz zuständigen Personen über die weiteren Schritte entscheiden, also ob man die Panne firmenintern lösen und die Behördenmeldung allein abgeben kann, oder ob man externe Unterstützung beizieht.

Im nächsten Beitrag sehen wir uns die folgenden Punkte näher an:
– Strafen, wenn Datenpanne nicht gemeldet wurde.
– Folgen einer Datenpanne, die durch falsche Bekanntgabe **vom Kunden ausgelöst** wurde.
– **Tipps** für die tägliche Praxis, um **Datenpannen weitestgehend vermeiden zu können.**

Weiterlese-Links:
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/

Quellen: Kurier, IVVA Webseite, Newsletter Meineberater.at, Webseite Datenschutzbeauftragter-DSGVO.com

ALLE bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen…
Oder kostenlos mit "JA zu INFO" an g.wagner@b2b-projekte.at anfordern.

Für Rückfragen:

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

Foto: Stephan Huger

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