Mag. Günter Wagner
B2B Projekte
für Finanz- und Versicherungsbranche

Datenpanne wegen zu vieler Empfänger unter AN oder CC anstatt BCC. Hätten Sie alles für eine Meldung binnen 72 Stunden bereit?

Heute greifen wir einen **aktuellen Anlassfall** auf, der sicher bei Ihnen auch schon mal passiert ist. Kürzlich erhielt ich von einem Unternehmen ein E-Mail und darin waren unter AN: rund **100 E-Mail-Adressen** sichtbar.

Zwar war der **Inhalt des E-mails relativ unbedeutend. Dennoch** liegt ein typischer Fall einer **Datenpanne vor.**
Konkret schrieb mir das Unternehmen, dass man Rechnungen nur noch bis zu einem bestimmten Datum annehmen würde. Mit einem Schlag hatte ich nun ganz offensichtlich die **Lieferantendatei** und zahlreiche persönliche Ansprechpartner in E-Mail-Form erhalten. Einige zwar als allgemeine Adressen, wie office@firmaxy.at, aber durchaus auch zahlreiche individuelle wie etwa guenter.wagner@firmaabc.at, womit auch **personenbezogene Daten** veröffentlicht wurden.

Wieder haben wir **Input vom auf Versicherungs- und Datenschutzrecht spezialisierten Anwalt Mag. Stephan Novotny eingeholt:**

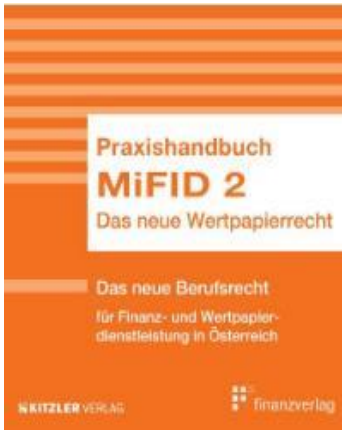
Im heutigen Beitrag beantworten wir Fragen wie:

- **Wann liegt eine Datenpanne vor?** Reicht schon das oben skizzierte **E-mail?**
- Muss es sich um **wichtigen Inhalt/Anhang handeln, um aktiv werden zu müssen?**
- Muss ich immer die **Behörde informieren?** Wenn Ja, wie schnell und wie genau?
- Wie wäge ich ab? Muss ich immer die **Betroffenen informieren?**
- Haben Sie einen **„Prozess“,** damit diese Tätigkeiten rasch und richtig erfolgen?

Die **bisher erschienen Praxis-Beiträge zur DSGVO von Mag. Novotny** können Sie hier nachlesen… oder **als PDF anfordern.** Ein mail mit Betreff JA zu Infos an g.wagner@b2b-projekte.at genügt.

Aktuelle Neu-Erscheinung:
Praxishandbuch MiFID 2, das neue Wertpapier-Recht!

Das neue Berufsrecht für Finanz- und Wertpapierdienstleistung.



Aktualisiert März 2021. Das bewährte (und um weitere Experten erweiterte) **Autorenteam** des **WAG-Handbuches** zeigt praxisorientiert im neuen Praxishandbuch auf, wie Ihr **Unternehmen die MiFID 2** umzusetzen hat.
ca. 900 Seiten, A5, Loseblatt, **EUR 106,-** (inkl. MWSt, exkl. Versand)

Bestellung/Rückfragen per mail an **g.wagner@b2b-projekte.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

Datenpanne wegen zu vieler Empfänger unter AN oder CC anstatt BCC. Hätten Sie alles für eine Meldung binnen 72 Stunden bereit?

Hier der Beitrag von Mag. Stephan Novotny:
Heute greifen wir einen **aktuellen Anlassfall** auf, der sicher bei Ihnen auch schon mal passiert ist.
Kürzlich erhielt ich von einem Unternehmen ein E-Mail und darin waren unter AN: rund 100 E-Mail-Adressen sichtbar.
Zwar war der Inhalt des E-mails relativ unbedeutend. Dennoch liegt ein typischer Fall einer Datenpanne vor.

Konkret schrieb mir das Unternehmen, dass man Rechnungen nur noch bis zu einem bestimmten Datum annehmen würde. Mit einem Schlag hatte ich nun ganz offensichtlich die **Lieferantendatei** und zahlreiche persönliche Ansprechpartner in E-Mail-Form erhalten. Einige zwar als allgemeine Adressen, wie office@firmaxy.at, aber durchaus auch zahlreiche individuelle wie etwa guenter.wagner@firmaabc.at, womit auch **personenbezogene Daten** veröffentlicht wurden.

Und wir erinnern uns auch an einen **Fall in Graz, wo Anfang September in einem Grazer Club** eine mit Corona-infizierte Person an einer Party teilnahm und dabei mehrere Mit-Gäste ansteckte. Daraufhin schrieb 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 auch hier irrtümlich die E-Mail-Adressen für alle sichtbar unter AN: anstelle unter BCC:

Übrigens: BCC ist die Abkürzung für Blind Carbon Copy und das bedeutet ein mit Kohlepapier erstellter Durchschlag. Soweit die Erklärung für unsere jüngeren Leser, die sich wohl nicht mehr an das Durchschlagpapier erinnern können, das man in Schreibmaschinen nutzte, um eine Kopie des Getippten zu erhalten.
Wann liegt einen Datenpanne vor?

War der Inhalt im oben geschilderten Fall eins eher belanglos, ist der Inhalt im zweiten Falle sehr bedenklich. Warum?

Einerseits teilte man 222 Personen öffentlich sichtbar mit, dass der Verdacht einer Corona-Erkrankung besteht. Also geht es hier um **Gesundheitsdaten** und diese zählen zu den **sensiblen**, d.h. besonders schützenswerten personenbezogenen Daten.

Außerdem hat dieser Fall möglicherweise auch eine **strafrechtliche Komponente.** Zur Erinnerung: Zu diesem Zeitpunkt waren Feiern nur mit maximal 200 Personen in geschlossenen Räumen erlaubt. Tatsächlich waren aber 222 Personen anwesend. Womit man also nun wusste, dass diese 221 Personen nicht nur womöglich Corona hatten, sondern auch das bestehende Gesetz übertreten hatten.

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

Häufige Fragen, die in diesem Zusammenhang immer wieder kommen:

> Liegt eine Datenschutzverletzung bereits dann vor, wenn ich ein E-Mail irrtümlich an viele Empfänger unter AN: also öffentlich sichtbar, sende?

> Oder liegt erst dann eine Datenschutzverletzung vor, wenn ich eine E-Mail etwa mit einem Anhang mit Kundendaten irrtümlich an einen falschen Empfänger absende?

> Oder liegt eine Datenschutzverletzung erst dann vor, wenn sensible (Religion, Gesundheit, sexuelle Orientierung, Gewerkschaftszugehörigkeit, etc.) oder zumindest finanzielle Daten wie IBAN, etc. drinnen stehen?

Antwort: Alle 3 skizzierten Fälle sind Datenpannen. Die Frage, in welchem Falle man was tun muss, ist schon schwieriger zu beantworten. Konkret geht es um die Frage, muss man die **Datenschutzbehörde und womöglich auch die betroffenen Kunden von der Panne informieren oder nicht.**

Gefahr: Gibt man keine Meldung ab und diese **wäre aber nötig** gewesen und ein Betroffener beschwert sich nachträglich oder die Behörde erfährt irgendwie anders von diesen Pannen, dann kann das teuer werden, denn die Betroffenen können **Schadenersatz** verlangen.

Dazu kommt, dass dann die **Datenschutzbehörde** das Unternehmen ganz besonders **genau prüfen** wird. Und die noch größere Gefahr ist wohl der **Image-Verlust,** 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 nachgesendet wird, in der man um das Löschung der ursprünglichen E-Mail ersucht. Allenfalls wird auch um eine Bestätigung der Löschung ersucht.

Die **gesetzlichen Regelungen zum Datenschutz kann diese Praxis nicht aushebeln,** schon gar nicht begibt man sich damit seiner Betroffenenrechte. Als marketingtechnische Reaktion des Verantwortlichen ist es aber sicherlich empfehlenswert. Und, sollte der Betroffene fälschlich bestätigen, das E-Mail gelöscht zu haben, und es kommt zu einem Databreach beim Betroffenen, so könnte auch diesen dann eine Schadenersatzpflicht treffen.

Wann Meldung, 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.**

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

Hier ein paar **Extrem-Beispiele**, die zeigen sollen, was ich meine:
Etwa: Durch ein offen versandtes E-Mail wird einer großen Zahl von Empfängern bekannt, dass man **Corona oder Aids oder sonst eine schwere, geächtete Krankheit** habe. Man kann sich wohl vorstellen, welche negativen Folgen das haben könnte (vielleicht Job-Verlust oder Ablehnung einer Bewerbung, soziale Ächtung durch das Umfeld, etc).

Ebenso wird niemand wollen, dass seine Adresse, seine **Kontodaten, Steuergeheimnisse,** usw. im Internet kursieren.
Oder: Ein unverschlüsselter USB-Stick mit allen möglichen **Firmendaten geht verloren**. Das sind wohl Fälle, wo jeder sagt, ja das ist eine Datenpanne, die müssen wir der Datenschutzbehörde melden.
Und dann gibt es wohl viele andere Fälle, wo die negativen Folgen der Datenpanne für die Betroffenen wohl nicht existent oder ganz gering sind.
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.**

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 die Panne nicht melden, weil sie es gesetzlich nicht müssen, legen Sie trotzdem einen **Aktenvermerk** an, beschreiben Sie darin, was passiert ist (etwa: E-Mail ging an 222 Empfänger öffentlich sichtbar) und was Sie getan haben, dass dies möglichst nicht mehr passieren sollte (Schulung des Verursachers oder der ganzen Abteilung, Mail mit anonymer Schilderung des Falles via Firmen-Rundmail, um das Problembewusstsein im ganzen Unternehmen zu steigern, die irrtümlich offen Angeschriebenen wurden neuerlich per Einzelmails kontaktiert, um Entschuldigung gebeten, etc.).

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 in dieser Meldung an die Behörde beschreiben Sie, was passiert ist und welche Maßnahmen Sie bereits gesetzt haben.

Wann Sie die Betroffenen informieren sollten, ist auch nicht einfach ganz allgemein zu beantworten.

Auch hier gilt es im Einzelfall abzuschätzen, welche Konsequenzen die Datenpanne hatte.

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

Wieder ein paar Extrembeispiele: Wenn etwa eine Urlaubsliste bekannt würde, könnte das die Gefahr von Einbrüchen bedeuten, wenn die Leute ins Ausland gefahren sind und die Wohnung unbeaufsichtigt ist. Oder eine veröffentlichte Liste mit Bankdaten könnte zu Hacker-Angriffen mit Geldverlusten zur Folge haben. Oder die Bekanntheit der Gewerkschaftszugehörigkeit könnte in Diktaturen zu Drohungen (oder noch Schlimmeren) führen. Die Bekanntgabe einer Krankheit könnte zu Jobverlust führen. Usw. usf. In solchen Fällen sind auf jeden Fall die Betroffenen zu informieren, damit sie sich gegen die Gefahren wappnen können.
Bei Unklarheiten sollten Sie auch hier juristischen Rat einholen.

Quellen: Ö1 Mittagsjournal, Interview mit Arge Daten zum Grazer-Fall, Newsletter von MeineBerater.at, medinlive.at, Datenschutz Vortrag bei AFPA durch Mag.a Birgit von Maurnböck

PS: Die Grazer Gesundheitsbehörde hat natürlich eine Meldung an die Datenschutzbehörde gemacht und die Betroffenen wurden von der Datenpanne schriftlich und telefonisch informiert.
beste Grüße von Mag. Stephan Novotny und Günter Wagner

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