PRESLMAYR
RECHTSANWÄLTE

PRESLMAYR
RECHTSANWÄLTE

IT-Rechtstag 27.5.2011

Data Breach Notification

Die Informationsplicht nach § 24 Abs 2a DSG

RA Dr. Rainer Knyrim

PRESLMAYR
RECHTSANWÄLTE

Teil 1

Praxisfälle

news 08.06.2006 13:53

heise Security

<< Vorige | Nächste >>

Datenklau könnte US-Regierung 26,5 Milliarden US-Dollar kosten

Nach dem Diebstahl einer externen Festplatte mit Millionen Datensätzen aktiver und ehemaliger US-Soldaten haben mehrere Kriegsveteranen-Verbände eine Sammelklage gegen das US-Department of Veterans Affairs (VA) eingereicht. Gemeinsam fordern die "Vietnam Veterans of America" (VVA), das "National Gulf War Resource Center", die "Radiated Veterans of America" sowie die Organisationen "Citizen Soldier" und "Veterans for Peace" 1000 US-Dollar Entschädigung für jede Person, die vom Datenklau betroffen ist.

Ein inzwischen gefeuerter Mitarbeiter des Ministeriums für Kriegsveteranen hatte die Festplatte entgegen den Dienstvorschriften mit nach Hause genommen. Bei einem Einbruch im Mai verschwand dann dieser Datenträger, der Namen, Geburtsdaten und auch Sozialversicherungsnummern enthält. Die US-Regierung räumt inzwischen ein, dass insgesamt 26,5 Millionen US-Bürger von dem Datendiebstahl betroffen sind. Darunter mehr als eine Million aktive Angehörige der Streitkräfte, Reservisten und Mitglieder der National Guards.

"Es ist ein Schrecken für alle Veteranen, zu wissen, dass vertrauliche Informationen über sie nun möglicherweise in die Hände von Leuten gefallen sind, die verheerende Schäden damit anrichten können", erklärte der Vorsitzende der "Vietnam Veterans of America", John Rowan. Nach Einschätzung von Sicherheitsexperten könnten ausländische Geheimdienste über die Daten die Adressen von Mitarbeitern des US-Militärs herausbekommen und gegen diese dann gezielt vorgehen. (pmz/c't)

news 29.12.2005 16:27

<< Vorige | Nächste >>

Hotelkette Marriott vermisst Backup-Bänder mit umfangreichen Kundendaten

Zum Jahresende meldet die Hotelkette Marriott die unschöne Entdeckung, dass in Orlando Backup-Bänder mit umfangreichen Daten von 206.000 Kunden abhanden gekommen sind, die Mitglieder des Marriott Vacation Club sind. Neben Adressdaten sollen auch Kreditkartendetails und Verdienstinformationen auf den Bändern gesichert worden sein. Alle Kunden seien angeschrieben worden, eine Versicherung stehe bereit, mögliche Schäden zu decken. Außerdem habe man einen Kreditbeobachtungsdienst engagiert, in dem sich Clubmitglieder einschreiben können.

Die nunmehr erfolgte Meldung von Marriott ist eine Pflichtmeldung, die in den USA erfolgen muss, sobald Kundendaten in Gefahr sind. Eine ähnliche Meldung musste vor wenigen Wochen die niederländische Bank ABN Amro veröffentlichen, nachdem ein Sicherungsband mit den Daten von zwei Millionen Kreditnehmern verschwunden war. Das Band sollte vom Transportunternehmen DHL zur Vermögensanalyse an einen Finanzdienstleister geliefert werden, ging aber unterwegs verloren. ABN Amro informierte daraufhin die Kunden, konnte aber vor wenigen Tagen das Mailing mit einer guten Nachricht wiederholen: Bei DHL wurde das vermisste Band gefunden.

Seit einiger Zeit warnen Datenschutzexperten wie Bruce Schneier davor, dass Firmen zu sehr auf ihre "Cyber-Security" achten und dabei den klassischen Datenschutz vernachlässigen. Viele Banken hätten es aufgegeben, Sicherungsbänder von eigenen Kurieren transportieren zu lassen. Auf den Trend haben die Transporteure auf ihre Weise reagiert: Sowohl Fedex als auch UPS schließen in ihren Geschäftsbedingungen inzwischen derart brisante Finanzdaten von ihren Versicherungsgarantien aus und empfehlen andere Transportformen. (*Detlef Borchers*) / (pmz/c't)

Version zum Drucken | Per E-Mail versenden << Vorige | Nächste >>

KURIER

UNABHÄNGIGE TAGESZEITUNG FÜR ÖSTERREICH

Wien
Dienstag, 13. Juni 2006
Nr. 161 / 0,90 €
www.kurier.at

HARTMANN AN DIE BURG
Matthias Hartmann wird Nachfolger von Burgtheaterchef Klaus Bachler. **SEITE 25**

AUF ZUM AUSVERKAUF
Die ersten Geschäfte haben bereits mit dem Sommer-Abverkauf begonnen. **SEITE 19**

Kurzeinsatz für den Größten

Geheimdaten aus Ministerium auf eBay versteigert

Gebrauchte Computer-Festplatte zum Verkauf angeboten: Vertrauliche Daten nicht richtig gelöscht

Honorarnoten, Werkverträge, „Informationen für den Vizekanzler" und Statistiken – im Online-Versteigerungshaus eBay wurde für 38,40 Euro eine gebrauchte Festplatte aus dem Verkehrsministerium versteigert, auf der sich Dutzende vertrauliche Dateien befunden haben. Laut Ministerium hätte die Festplatte von einer Firma verschrottet werden müssen, wurde aber von einem Mitarbeiter abgezweigt. **SEITE 23**

Ministeriums-Festplatte auf eBay verkauft

KURIER EXKLUSIV Dutzende vertrauliche Unterlagen und Statistiken konnten rekonstruiert werden

VON GERALD REISCHL

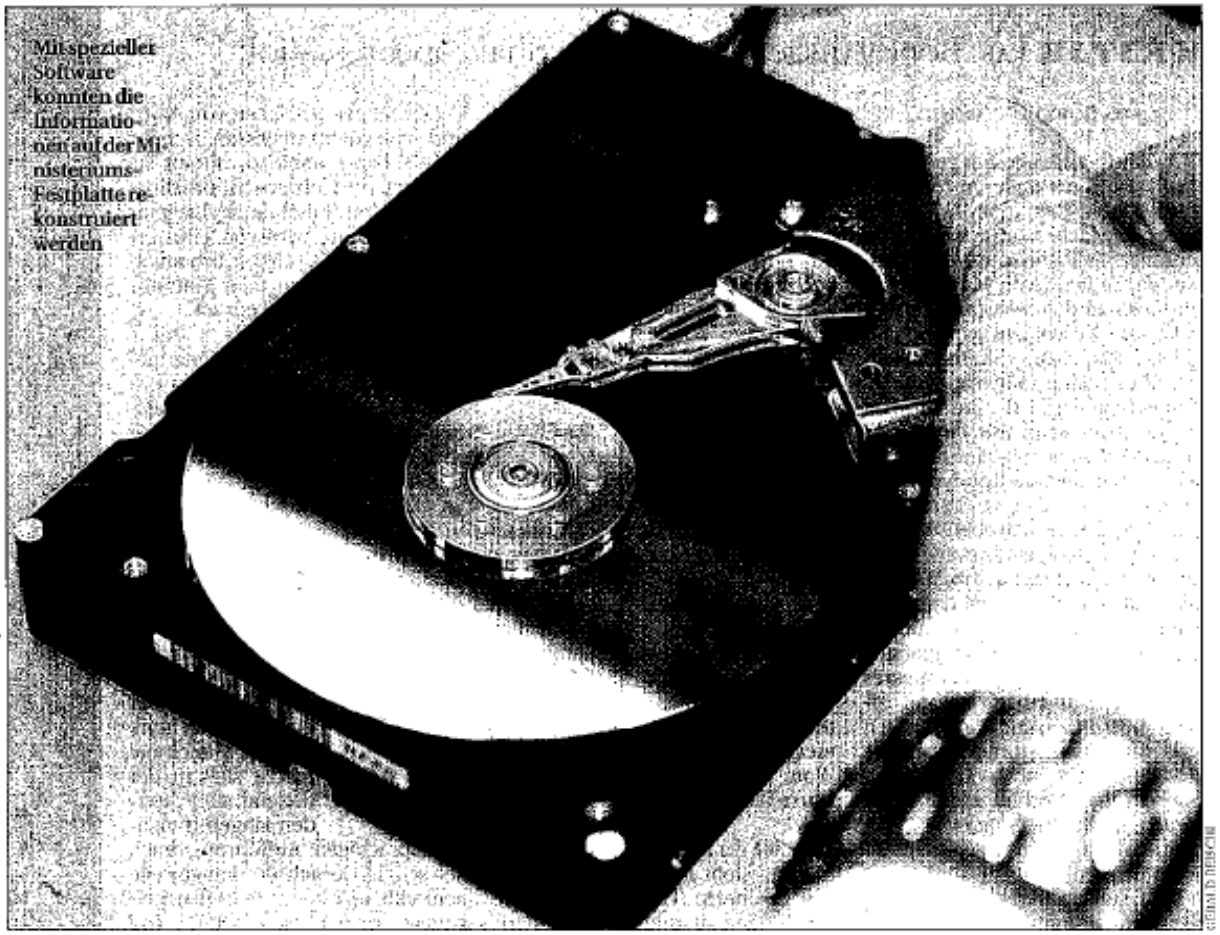
Honorarnoten, Werkverträge, Excel-Dateien mit der exakten Einnahmeentwicklung aus den Wunschkennzeichen, diverse „Informationen für den Herrn Vizekanzler", und Budget-Controlling-Berichte – eine Festplatte mit vertraulichen Informationen aus dem *Bundesministerium für Verkehr, Infrastruktur und Technologie* (BMVIT) ist im April auf eBay versteigert worden. Während das Ministerium derzeit prüft, wie die Festplatte auf eBay gelangen konnte, sind IT-Experten überzeugt, dass immer wieder gebrauchte Festplatten mit privaten, Firmen- und Behördendaten in Versteigerungshäusern, Flohmärkten und Computer-Secondhand-Geschäften „unters Volk gebracht werden".

„Es ist unverantwortlich, Festplatten vor dem Weiterverkauf nicht richtig zu löschen."
DATENRETTER ENGELLAND

DIE VORGESCHICHTE Für eine Reportage über den Handel mit gebrauchten Festplatten kaufte der KURIER 30 Festplatten an und ließ sie im Labor des deutschen Datenrettungs-Unternehmens KrollOntrack (*www.krollontrack.at*) analysieren. Von den 30 Festplatten waren zwar zehn völlig defekt, auf 20 konnten aber die darauf befindlichen Daten rekonstruiert werden. Zum Teil genügte der einfache Einbau in einen Rechner, um an die Daten zu gelangen, teilweise wurde ein Datenrettungs-Programm genutzt.

GEHEIM Die Analyse einer der Festplatten, einer *Maxtor 20 GB 3,5 Zoll Desktop* ergab schließlich, dass diese bis Herbst 2005 in der *Abteilung II/FC – Finanzen und Controlling* des BMVIT im Einsatz gewesen sein musste – die meisten der darauf befindlichen Informationen konnten direkt dieser Abteilung zugeordnet werden.

FORMATIERT „Die Festplatte war zwar formatiert, allerdings konnten wir mit unserer Datenrettungssoftware die Informationen auf der Platte wieder rekonstruieren", sagt der Chef des Datenrettungslabors bei KrollOntrack, Holger Engelland. Solche Programme gibt es bereits ab 95 € für jedermann zu kaufen. Engelland: „Das Formatieren einer Festplatte reicht nicht aus, damit Daten endgültig gelöscht werden." (siehe Kasten unten).



Mit spezieller Software konnten die Informationen auf der Ministeriums-Festplatte rekonstruiert werden

Formatieren & Löschen: Das Festplatten-ABC

Format Um eine Festplatte nutzen zu können, muss diese *formatiert* werden. Grundsätzlich gibt es

Achtung Irrglaube ist, dass durch das Formatieren Daten gelöscht werden. Meist verbleiben die Da-

Bescheid wissen müsste, will sich auf Grund dieses Vorfalls künftig bei der Entsorgung von Computer-Hardware selbst kümmern. „Wir haben eine eigene Magnetisierungs-

Sony-Datendiebstahl: Klagen auch in Österreich möglich

Der Diebstahl sensibler Daten von Millionen Onlinenutzern der Sony PlayStation könnte auch die österreichischen Zivilgerichte beschäftigen. Denn österreichische Konsumenten hätten die Möglichkeit, bei Schäden Sony in Österreich zu klagen, so die Einschätzung des Wiener Rechtsanwalts Rainer Knyrim von der Wirtschaftskanzlei Preslmayr gegenüber der APA.

Er glaubt aber, dass betroffene Kreditkartenbesitzer im Falle von Ungereimheiten durch Kreditkartenunternehmen bzw. Sony entschädigt würden. Das erfolge meist im Wege einer außergerichtlichen Einigung, ohne dass geklagt werden müsse, so der Anwalt.

Österreichische Mindeststandards garantiert

Mit den Usern vereinbarte Sony zwar generell englisches Recht, aufgrund europäischer Normen sei aber sichergestellt, dass österreichische Mindeststandards im Konsumentenschutzbereich gelten. Sollten die Kreditkartendaten von Millionen Usern unverschlüsselt gewesen sein, dann wäre das ein „grober Sicherheitsverstoß“, so Knyrim weiter.

PRESLMAYR
RECHTSANWÄLTE

Teil 2

Informationspflicht nach

§ 24 Abs 2a DSG

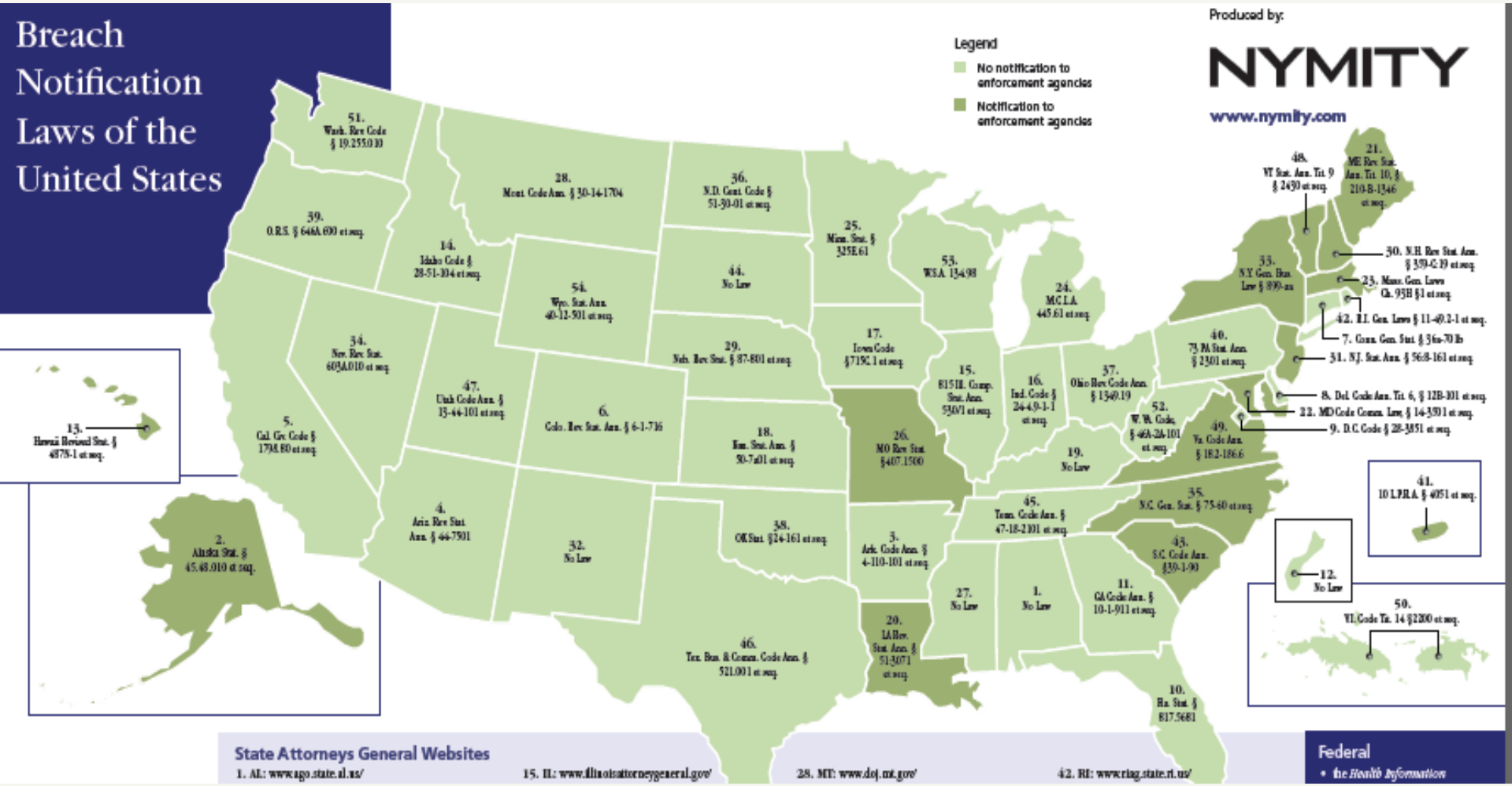
Entwicklung der Data Breach Notification

- Entwicklung aus USA, zunächst über England in EU gekommen.

- In USA bereits ein eigener Wirtschaftszweig. Unterschiedliche Formen der Benachrichtigung verpflichtend, von individuellen Anschreiben bis Inserate und TV-Spots mit Aufrufen, sich auf Hotline zu melden. Meist Datenschutz-Behörde zu informieren

PRESLMAYR
RECHTSANWÄLTE

Gesetzliche Vorschriften zur DBND in den USA



Data Breach Notification

- Auf EU-Ebene diskutiert, erstmalig in neuer RL zur elektronischen Kommunikation enthalten (e-privacy – RL). Neue Datenschutz-Kommissarin in Brüssel ist alte Telekom-Kommissarin Viviane Reding, die e-privacy-RL umgesetzt wird. Daher rechnet man auf EU-Ebene und auf Ebene der Datenschutzbehörden damit, dass auch in Datenschutz-RL demnächst Data Breach Notification hineinkommt.

- Österreich neben Deutschland Vorreiter bei der Einführung in der EU

Regelung in Deutschland seit 1.9.2010

- Neuer § 42a BDSG: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten
- Eingeschränkt auf bestimmte, besonders „heikle“ Datenarten: Sensible Daten, Berufsgeheimnisdaten, Daten über strafbare Handlungen, **Bank- und Kreditkartenkontendaten**
- Aufsichtsbehörde und Betroffene sind unverzüglich zu informieren
- Wenn Benachrichtigung unverhältnismäßiger Aufwand, insbes. wegen Vielzahl der Betroffenen, stattessen Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens 2 bundesweit erscheinenden Tageszeitungen oder durch andere gleich wirksame Maßnahme. (Kritik: 1 solches Inserat kostet rd. EUR 30.000,--!)

§ 25 Abs 2a DSG 2000

- per 1.1.2010 mit der Datenschutzgesetz-Novelle 2010 eingeführt
- Österreich nimmt Vorreiterrolle ein

- **Tatbestandsvoraussetzungen:** erster Satz

- **spezielle Befreiungstatbestände:** zweiter Satz

PRESLMAYR RECHTSANWÄLTE

§ 25 Abs 2a DSG 2000

- *„Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen **systematisch und schwerwiegend unrechtmäßig verwendet** wurden und den Betroffenen **Schaden droht**, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. **Diese Verpflichtung besteht nicht**, wenn die Information angesichts der Drohung eines nur **geringfügigen** Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen **unverhältnismäßigen Aufwand** erfordert.“*

Tatbestandvoraussetzungen

- **„Daten wurden s*ystematisch, schwerwiegend und unrechtmäßig verwendet* “**
- Auch manuelle Daten sind erfasst!
- „***Systematisch***“
  - Unbestimmter Rechtsbegriff
  - Gegenteil von „zufällig“?
  - Zeitliche Komponente?

Tatbestandvoraussetzungen

- **„Daten wurden s*ystematisch, schwerwiegend und unrechtmäßig verwendet* “**
- „***schwerwiegend***“
  - Unbestimmter Rechtsbegriff
- „***unrechtmäßig***“
  - Jegliche Verwendung entgegen den Bestimmungen des DSG (insb §§ 6 ff)

Tatbestandvoraussetzungen

- **„Daten wurden s*ystematisch, schwerwiegend und unrechtmäßig verwendet* “**
- „***wurden verwendet*** “ (Passiv)
  - Neutrale Formulierung
  - Auslöser kann neben einem unredlichen Dritten auch der Auftraggeber selbst, einer seiner Mitarbeiter, sein Dienstleister oder ein technisches Gebrechen sein
- „**verwenden**“
  - § 4 Z 8 – Z 12: Jede Art der Handhabung von Daten (in der Praxis ist schon das Kopieren, Abfragen, Ausdrucken, Übermittlung relevant)
  - fahrlässiges Verlieren fällt wohl nicht unter den Wortlaut

PRESLMAYR
RECHTSANWÄLTE

Tatbestandvoraussetzungen

- **Es droht ein Schaden, der mehr als geringfügig ist**
  - Einschränkung auf bloße Vermögensschäden oder auch immaterieller Schaden?
  - Ein Schaden muss noch nicht eingetreten sein, es reicht die bloße Möglichkeit, es muss aber ein Schaden drohen
  - Allgemeines Zivilrecht: Schadensminderungspflicht

PRESLMAYR RECHTSANWÄLTE

Problem: Form der Informationspflicht

- Auf welche Art und Weise die Information der Betroffenen zu erfolgen hat, legt der Gesetzgeber nicht fest.
- Nach der Eignung zu beurteilen (zB: Brief, Telefon, Email, Webseite, Veröffentlichung in Tageszeitung).
- Detailgrad und Inhalt der Information nicht geregelt.
- Die DSK ist nicht zu informieren.

Erster Befreiungstatbestand

- dem Betroffenen droht nur ein „***geringfügiger Schaden***“
  - Unbestimmter Rechtsbegriff
  - Denkbar: individuelle Beurteilung je nach Betroffenengruppe

Zweiter Befreiungstatbestand

- Frage: und/oder? = oder (alternativ, nicht kumulativ)
- „***die Kosten der Information aller Betroffenen erfordern einen unverhältnismäßigen Aufwand***“
  - Interessensabwägung erforderlich
  - Problem: wie ist die Verhältnismäßigkeit festzustellen? zB: Inserat in Kronen Zeitung ½ Seite kostet ca. EUR 25.000,--.

PRESLMAYR
RECHTSANWÄLTE

Was tun im „worst case“?

- Was kann ein Unternehmen tun, wenn zufällig Daten verloren gehen und von Drittem gefunden werden?
- 1. Schritt: Welche Daten sind betroffen?
- 2. Schritt: Welche Personen haben Zugang zu den Daten erlangt?
  - Eidesstattliche Erklärungen einholen über Datenverwendung
  - Problem bei Medien: Redaktionsgeheimnis
- 3. Schritt: Ist eine Löschung der Daten möglich?
  - IT-Forensik muss untersuchen und löschen.
  - Wichtig: Bestätigung der Löschung
- 4. Schritt: Wenn keine Löschung aller Daten möglich: Rechtliche Prüfung, ob Informationspflicht vorliegt
- 5. Schritt: Information durchführen

PRESLMAYR
RECHTSANWÄLTE

Was tun im „worst case“?

- Ziel der Maßnahmen: Schadensminimierung bzw Schadenseintrittsverhinderung!
- So kann möglicherweise die Informationspflicht vermieden werden!
- Vorsorge ist besser als Nachsorge: Notfallplan für „zufälligen“ Datenverlust konzipieren!

Vorbereitung für Ernstfall (1)

- Prozessablauf inkl. rechtliche Prüfung vorplanen, Checklisten erstellen
- Eventuell Vorprüfung konkret möglicher Szenarien
- Muster für Informationsschreiben an Betroffene entwerfen, andere Informationsszenarien vorplanen (Vorfälle für Mitarbeiterdaten und Kundendaten)

Vorbereitung für Ernstfall (2)

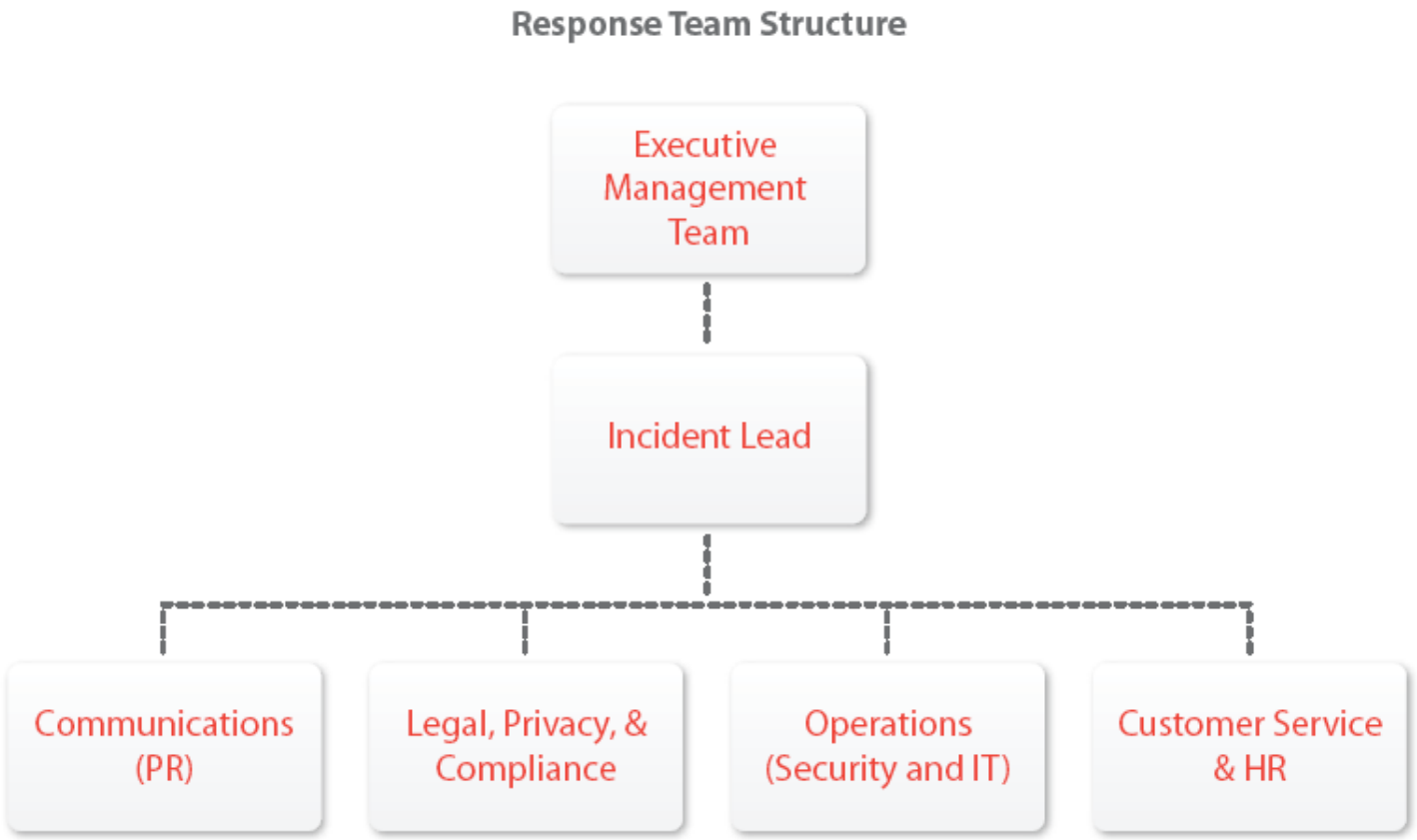
- Dokumentationsunterlagen über Vorfälle erstellen, um Dokumentation im Ernstfall für Beweiszwecke sicherzustellen

- Derzeitige eigene Versicherungsbedingungen auf mögliche Haftungsfreizeichnung prüfen.

- Eigene Datenanwendungen rechtlich prüfen und formelle datenschutzrechtliche „Hausaufgaben“ machen, um sich nicht Vorwurf aussetzen zu müssen, man habe seine Pflichten nicht erfüllt. – DVR ab Juli Online! = einfacher zusätzlicher Stoff für Skandalgeschichten

PRESLMAYR
RECHTSANWÄLTE

Schaffung einer Response Team Struktur



USA: Credit Monitoring and Alerts (z.B. in USA)

- Dieser Dienst überwacht Änderungen der individuellen Datensätze gemeinsam mit einem der nationalen Kredit-Auskunft-Institutionen (Kredit-Abteilungen).
- Die Mitglieder werden über jede Veränderung ihrer Aufzeichnungen, einschließlich der neu eröffneten Konten oder eine Veränderung Kredit-Bedingungen umgehend benachrichtigt.

USA: Automated Fraud Alerts – Automatischer Kontrollanruf bei Kreditbeantragung

- Bei Kreditbeantragung im Namen eines Mitglieds erfolgt standardmäßig ein Kontrollanruf, um die Beantragung bestätigen oder stornieren zu lassen
- Mitglieder erhalten regelmäßig Auskunft über Kreditwürdigkeit und aktuelle Kreditguthaben von allen großen Kreditbüros, inklusive einer zusammengefassten Kreditanalyse
- Beispiel, dass in diese Richtung geht: Security SMS – Service von Diners Club

Der wirtschaftliche Aspekt

Studie der Universität Utah für 2008:

- Durchschnittliche Gesamtkosten eines Data Breach in den USA waren 2008 USD 6,65 Millionen
- Durchschnittliche Kosten pro Betroffenem waren USD 202,-- (beinhaltet Kostenübernahme für Credit-Monitoring)
- Kosten pro Betroffenem bei böswilligem Angriff waren USD 225,--, bei fahrlässigem Datenverlust nur USD 199,--.
- Kosten pro Betroffenem, wenn Fall durch verlorenen oder gestohlenen Laptop ausgelöst wurde, waren USD 249,--, bei Fällen ohne Laptop nur USD 177,--.
- Wenn es der erste Fall war, waren die Kosten pro Betroffenem USD 243,--, wenn es der zweite Fall beim selben Unternehmen war, nur noch USD 192,-

(Quelle: Vortrag von Chris Kidd, Chief Information Privacy & Security Officer, Universität Utah am IAPP Summit, Washington, März 2009).

PRESLMAYR
RECHTSANWÄLTE

Teil 3

Konsequenzen

PRESLMAYR
RECHTSANWÄLTE

Liechtenstein: Bank entschädigt deutschen Steuersünder (ORF, 8.2.2010)

Eine frühere Tochtergesellschaft der Liechtensteiner Fürstenbank LGT muss einem Bericht zufolge **einem deutschen Steuersünder 7,3 Mio. Euro Entschädigung zahlen**.

Nach Informationen der "Süddeutschen Zeitung" fällte das fürstliche Landgericht in Liechtenstein ein entsprechendes Urteil. Darin heiße es, dass die damalige LGT-Treuhand AG **den Kläger zu spät darüber informiert habe, dass seine Kundendaten und die von mehreren hundert anderen Deutschen gestohlen worden waren**.

Der Datendieb war ein früherer Mitarbeiter, der die CD mit den Daten für 4,5 Mio. Euro dem deutschen Bundesnachrichtendienst verkauft hatte. Dadurch war vor zwei Jahren unter anderen Deutsche-Post-Chef Klaus Zumwinkel als Steuersünder aufgeflogen.

Weitere Klagen erwartet
Weil mehrere Deutsche ähnliche Klagen planen, sei das Urteil mit Spannung erwartet worden, schreibt die Zeitung. Die Argumentation der enttarnten Steuersünder ist demnach im Wesentlichen dieselbe: **Hätte die LGT Treuhand sie unverzüglich über den Datenklau informiert, hätten sie sich selbst beim deutschen Fiskus anzeigen oder von einer zeitweiligen Amnestie profitieren können**. **Dadurch wären sie mit geringeren Geldstrafen weggekommen, als das nach ihrer Enttarnung der Fall ist**.

Das fürstliche Landgericht in Vaduz bewertete das dem Bericht zufolge ähnlich und gab damit dem Kläger recht.

LGT legt Berufung ein
Das Urteil ist nicht rechtskräftig, da die LGT Treuhand AG Berufung angekündigt hat. LGT habe erst im Februar 2008 einen Zusammenhang zum Datendiebstahl von 2002 herstellen können, heißt es in einer Mitteilung der AG. Die im Urteil erwähnten Anhaltspunkte für eine Datenweitergabe, die bereits im Herbst 2007 bekanntgeworden sein sollen, seien somit nicht richtig.

Der zivilrechtliche Aspekt (1)

- Data Breach Notification dient der Schadensminimierung.
- Die Pflicht zur Schadensminimierung ergibt sich im Zivilrecht aus dem ABGB auf zwei Arten:

1. Aus dem direkten Verschulden, dem Vorsatz: Vorsätzlich handelt, wem die Rechtswidrigkeit seines Handeln bewußt ist, wer den schädlichen Erfolg vorhersieht und seinen Eintritt billigt. – Bewußtes Negieren der Informationspflicht der Betroffenen, wenn ein Datenschutzleck entstanden ist könnte daher per se als eigenständiges rechtswidriges Handeln gesehen werden, selbst wenn das Unternehmen ursprünglich „Opfer“ eines Dritten (zB Hackers) wurde.

Der zivilrechtliche Aspekt (2)

2. Wenn man das Unternehmen nur als Opfer sieht, so hat es eine Schadensminderungspflicht, die aus § 1304 ABGB abgeleitet wird: Es ist die Pflicht des Geschädigten, dem unmittelbar drohenden Eintritt des Schadens oder seiner Vergrößerung möglichst entgegenzuwirken. – Information der Betroffenen ist daher erforderlich.

- DBN ist daher vor allem auch Thema für die Versicherung des Unternehmens, die die Einhaltung der Informationspflicht prüfen wird und bei Nichteinhaltung die Deckung versagen wird, entweder wegen vorsätzlicher Nichtinformation der Betroffenen durch das versicherte Unternehmen oder wegen mangelnder Schadensminderung. Der neue § 24 Abs 2a DSG 2000 hilft der Versicherung bei dieser Information bestens, da jeweils vom versicherten Unternehmen gegen eine gesetzliche Verpflichtung (Schutzgesetz iSd § 1311 ABGB) verstoßen wird, wenn diese nicht eingehalten wird!

Zivilrechtliche Konsequenzen

Für einen Auftraggeber (Bsp Unternehmen)

- Deliktischer Schadenersatz
  - §§ 1,33 DSG iVm § 1311 ABGB
  - *Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. (§ 33 DSG)*
  - *Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. (§ 1 DSG)*

Strafrechtliche Konsequenzen

Für einen Auftraggeber (Bsp Unternehmen)

- **Verbandsverantwortlichkeitsgesetz (VbVG)**
- Definition „Verband“: Alle juristischen Personen sowie Personengesellschaften
- Unternehmen haftet für gerichtlich strafbare Tatbestände von:
  - *Entscheidungsträgern*, wenn diese die Tat rechtswidrig und schuldhaft begangen haben.
  - *Mitarbeitern*, wenn diese die Tat rechtswidrig und schuldhaft begangen haben und die Begehung der Tat dadurch ermöglicht oder wesentlich erleichtert wurde, dass Entscheidungsträger die nach den Umständen gebotene und zumutbare Sorgfalt außer Acht gelassen haben, insbesondere indem sie wesentliche technische, organisatorische oder personelle Maßnahmen zur Verhinderung solcher Taten unterlassen haben.

PRESLMAYR
RECHTSANWÄLTE

Strafrechtliche Konsequenzen

Für einen Auftraggeber (Bsp Unternehmen/Bank)

- Strafe = „Verbandsgeldbuße“
- Strafhöhe: bis zu 180 Tagessätze, Tagessatz = 1/360 des Jahresertrages + max. 30%.
- Maximaler Tagessatz = € 10.000.—
- Höchststrafe somit: € 1,8 Mio!!
- Verhinderung: § 14 DSG - Datensicherheitsmaßnahmen!

Konsequenzen des Dritten, der Daten „findet“

- **Zivilrechtliche Verantwortlichkeit**
- Als Grundlage für einen deliktischen Schadenersatzanspruch bleibt nur §§ 1, 33 iVm § 1311 ABGB
- **Strafrechtliche Verantwortlichkeit: § 51 DSG**
- *Wer mit dem **Vorsatz**, sich oder einen Dritten dadurch unrechtmäßig zu **bereichern**, oder mit der **Absicht**, einen anderen dadurch in seinem von § 1 Abs 1 gewährleisteten Anspruch zu **schädigen**, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung **anvertraut oder zugänglich geworden sind** oder die er sich **widerrechtlich verschafft** hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, **wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.***

Verwaltungsrechtliche Konsequenzen: § 52 DSG

- **§ 52 ist subsidiär** (vgl Abs 1: „*Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist“)*
- *Geldstrafe bis zu 25 000 Euro*
- **Im gegenständlichen Fall relevante Tatbestände** – *zu bestrafen ist, wer*
  - *Z 1: sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder*
  - *Z 2: Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet*

PRESLMAYR
RECHTSANWÄLTE

Teil 4

Ausblick: Data Breaches („Sicherheitsverletzungen“) im TKG

PRESLMAYR RECHTSANWÄLTE

Novelle des TKG 2003 - 269 ME XXIV. GP

- **§ 95a neu**: „Sicherheitsverletzungen“
- **Abs 1**: „***Im Fall einer Verletzung des Schutzes personenbezogener Daten hat*** *unbeschadet des § 16a* ***der Betreiber öffentlicher Kommunikationsdienste unverzüglich die Datenschutzkommission von dieser Verletzung zu benachrichtigen****. Ist anzunehmen, dass durch eine solche Verletzung Personen in ihrer Privatsphäre oder die personenbezogenen Daten selbst beeinträchtigt werden, hat der* ***Betreiber auch die betroffenen Personen unverzüglich von dieser Verletzung zu benachrichtigen***.“

Novelle des TKG 2003 - 269 ME XXIV. GP

- **§ 95a neu**: „Sicherheitsverletzungen“
- **Abs 2:** „*Der Betreiber öffentlicher Kommunikationsdienste kann von einer Benachrichtigung der betroffenen Personen* ***absehen****, wenn der Datenschutzkommission nachgewiesen wird, dass er* ***geeignete technische Schutzmaßnahmen*** *getroffen hat und dass diese Maßnahmen* ***auf die von der Sicherheitsverletzung betroffenen Daten angewendet worden sind****. Diese technischen Schutzmaßnahmen müssen jedenfalls sicherstellen, dass die Daten die Daten für unbefugte Personen verschlüsselt sind.*“

PRESLMAYR RECHTSANWÄLTE

Novelle des TKG 2003 - 269 ME XXIV. GP

- **Abs 3:** „*Unbeschadet der Verpflichtung des Betreibers nach Abs. 1 zweiter Satz **kann die Datenschutzkommission** den Betreiber öffentlicher Kommunikationsdienste – nach Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung – auch **auffordern**, eine Benachrichtigung durchzuführen*."

- **Abs 4:** „*In der Benachrichtigung an die betroffenen Personen sind jedenfalls die **Art der Verletzung** des Schutzes personenbezogener Daten **zu beschreiben**, **Kontaktstellen** zu nennen, bei denen weitere Informationen erhältlich sind, und **Maßnahmen** zur Begrenzung der möglichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten **zu empfehlen**. In der Benachrichtigung an die Datenschutzkommission sind zusätzlich die **Folgen** der Verletzung des Schutzes personenbezogener Daten und die vom Betreiber öffentlicher Kommunikationsdienste nach der Verletzung vorgeschlagenen oder ergriffenen Maßnahmen darzulegen.*"

Novelle des TKG 2003 - 269 ME XXIV. GP

- **Abs 5:** „*Nähere **Einzelheiten**, insbesondere Form, Verfahrensweise oder Voraussetzungen für die Benachrichtigung bei einer Sicherheitsverletzung, kann der **Bundeskanzler** durch **Verordnung** festlegen. Die Datenschutzkommission kann im Einzelfall auch entsprechende Anordnungen treffen, um eine den Auswirkungen der Sicherheitsverletzung angemessene Benachrichtigung der betroffenen Personen sicherzustellen. Sie kann auch Leitlinien im Zusammenhang mit Sicherheitsverletzungen erstellen.*“

- **Abs 6: „*Die Betreiber öffentlicher Kommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen**. Es hat Angaben zu den Umständen der Verletzungen, zu deren Auswirkungen und zu den ergriffenen Abhilfemaßnahmen zu enthalten und muss geeignet sein, der Datenschutzkommission die Prüfung der Einhaltung der Bestimmungen gemäß Abs. 1 bis 4 zu ermöglichen*.“

Novelle des TKG 2003 - 269 ME XXIV. GP

- **Abs 7:** „*Die Datenschutzkommission hat die Regulierungsbehörde über jene Sicherheitsverletzungen zu informieren, die für die Erfüllung der der Regulierungsbehörde durch § 16a übertragenen Aufgaben notwendig sind.*“
- Erläuterungen zum Ministerialentwurf:
  - Umsetzung der Art. 4 Abs. 3 und 4 DatenschutzRL für elektronische Kommunikation
  - Während für Gefahren, die mit der Sicherheit des Netzbetriebes, also der Infrastruktur in Verbindung stehen, die Regulierungs-behörde zuständig ist, ist für Verletzungen, die personenbezogene Daten betreffen, die Datenschutzkommission zuständig. Dazu besteht auch eine gegenseitige Informationsverpflichtung.

Novelle des TKG 2003 - 269 ME XXIV. GP

- Abgrenzungsproblematik:

1. Zwischen § 24 Abs 2a DSG und § 95a neu TKG: Wann ist welche Bestimmung anzuwenden? zB: Was wenn TK-Betreiber Laptop mit Kreditkartendaten von Kunden oder Mitarbeitern verliert – fällt das unter TKG, weil Laptop von TK-Betreiber stammt, obwohl es vielleicht nichts mit TK-Dienst zu tun hat? Konsequenz vor allem: Einschaltung der DSK oder nicht?

2. Im Fall des § 95a neu TKG: Zwischen Regulierungsbehörde (Gefahren iVm Sicherheit des Netzbetriebes) und DSK (personenbezogene Daten). zB: Hacker hackt Standortdaten aus Handys: = personenbezogen, hat aber auch mit Netzbetrieb zu tun.

Ende

Vielen Dank für die Aufmerksamkeit!

RA Dr. Rainer Knyrim, Preslmayr Rechtsanwälte OG

1010 Wien, Dr. Karl Lueger-Ring 12

Tel. +43/1/5331695, Fax +43/1/5355686, knyrim@preslmayr.at

Literatur + Newsletter: www.preslmayr.at/datenschutz.php