ARGE DATEN

ARGE DATEN - Österreichische Gesellschaft für Datenschutz

vorab per Fax: +43.1.52152.2829

Unser Zeichen: brief-ortner-20110304.doc

Frau
Bundesminister Mag[a]. Claudia Bandion-Ortner
BM FÜR JUSTIZ (BMJ)

Museumstraße 7
A-1070 WIEN
Einschreiben, Rückschein

Wien, 4. März 2011

Betreff: Rechtswidrige Abfragen/Verwendung von Exekutionsdaten

Sehr geehrte Frau Bundesminister Bandion-Ortner!

Im Zusammenhang mit den nunmehr auch aktenkundigen rechtswidrigen Abfragen und Weitergaben von Exekutionsdaten, darf ich darauf hinweisen, dass es sich dabei nicht um einzelne Verfehlungen einzelner Beamter handelt, sondern dass bestimmte Wirtschaftsauskunftsdienste, zuletzt die Firma Deltavista, über lange Jahre und flächendeckend Exekutionsdaten zur Bonitätsbeurteilung angeboten und auch verkauft haben. Dabei wurde ausdrücklich auf den amtlichen Charakter dieser Daten hingewiesen, d.h. dass diese Daten aus amtlichen (gerichtlichen) Quellen stammen und daher besonders aussagekräftig seien.

Deltavista selbst hat auf seiner Website die seit 2005 bestehende Zusammenarbeit mit jenem Unternehmen veröffentlicht, dass schon seit Jahren Exekutionsdaten weiter verbreitet.

Die ARGE DATEN hat in den letzten zehn(!) Jahren mehrfach auf die Missstände im Zusammenhang mit den Exekutionsdaten hingewiesen und 2007 auch eine entsprechende Anzeige bei der Staatsanwaltschaft Wien eingebracht. Diese wurde zwar unter der Aktenzahl GZ 140 BAZ 3817/07d protokolliert, jedoch nach über einem Jahr wurde die Anzeige zurückgelegt.

Auf Grund verschiedener Aussagen handelt es sich um mehrere Millionen Datensätze, die bis zu zwei Millionen BürgerInnen betreffen können. Diese Bürger hatten durch diesen Datenhandel - in vielen Fällen völlig zu unrecht -, jedenfalls jedoch rechtswidrig schwere wirtschaftliche Schäden zu tragen.

Möglich wurde die jahrelange und flächendeckende widmungswidrige Nutzung der Exekutionsdaten durch offenbar völliges Fehlen von Sicherheits- und

Protokollierungsmaßnahmen, wie sie § 14 DSG 2000 zwingend für jeden Auftraggeber, also auch das Justizministerium, vorschreibt.

Weiters verlangt § 24 Abs. 2a DSG 2000 zwingend die Verständigung aller potentiell Betroffener, wenn ihnen durch eine Datenschutzverletzung Schaden droht. Ich darf darauf hinweisen, dass diese Informationspflicht nicht zwingend eine gerichtlich strafbare Handlung voraussetzt, sondern schon dann gegeben ist, wenn Daten aus technischen oder sonstigen administrativen Gründen unrechtmäßig verwendet werden.

Ich ersuche Sie daher um Beantwortung folgender Fragen:

1) Wann werden Sie alle von der Datenweitergabe Betroffenen über die Tatsache der Datenweitergabe gemäß § 24 Abs. 2a DSG 2000 informieren?
2) In welcher Form werden Sie die Betroffenen informieren?
3) Sollte eine Information unterbleiben, womit begründen Sie diese fehlende Information?
4) Wird es für betroffene Personen ein Angebot zur Verfahrensunterstützung geben, etwa zur Durchsetzung von Löschungs- und Schadenersatzansprüchen nach §§ 27 und 33 DSG 2000?
5) Wenn nein, wie begründen Sie dieses fehlende Angebot? Immerhin wurden durch fehlende Sicherheits- und Aufsichtsmaßnahmen des Justizministeriums erst diese langdauernden Datenweitergaben ermöglicht?
6) In welchem Umfang haben Sie finanzielle Vorsorge für allfällige Amtshaftungsforderungen gegen die Republik bzw. das Justizministerium getroffen?
7) Aus welchen Gründen wurde die Anzeige 140 BAZ 3817/07d aus dem Jahr 2007 zurückgelegt und das Verfahren eingestellt, obwohl schon in dieser Zeit Exekutionsdaten des Justizministeriums von Wirtschaftsauskunftsdiensten massiv missbraucht wurden?
8) Welche Protokollierungs- und Sicherheitsmaßnahmen im Sinne § 14 DSG 2000 waren bei der Exekutionsdatenbank bis Ende 2010 im Einsatz?
9) Wie wurde deren Einhaltung überwacht und wie wurde sichergestellt, dass die Verpflichtungen nach § 14 Abs. 2 Z 7 DSG 2000, die Überwachung der tatsächlich durchgeführten Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden konnten?
10) In welchem Umfang (wie oft und wieviele Abfragen betreffend) wurde bis Ende 2010 (insbesondere während Ihrer Amtszeit) eine Überprüfung im Sinne § 14 Abs. 2 Z 7 DSG 2000 durchgeführt?
11) Welche neuen (zusätzlichen) Sicherheitsmaßnahmen gemäß § 14 DSG 2000 werden seit Jahresbeginn bzw. in naher Zukunft gesetzt um Missbräuche frühzeitig zu erkennen und abzustellen?
12) Welche zusätzlichen proaktiven Maßnahmen werden Sie setzen, um unplausible Abfragen und Datenweitergaben schon frühzeitig zu erkennen und abzustellen?
13) Wird das österreichische Sicherheitshandbuch (https://www.sicherheitshandbuch.gv.at/), dass gemäß eines Beschlusses des Ministerrats alle Bundesdienststellen bei IT-Anwendungen verwenden sollen, in Ihrem Ressort vollständig und für alle Datenanwendungen angewendet?

14) Welche unabhängige (externe) Stelle überwacht die Einhaltung der Vorgaben des Sicherheitshandbuches?

Ich ersuche Sie um möglichst kurzfristige Beantwortung und habe mir den 20. März 2011 als Eingangsdatum Ihrer Antwort vorgemerkt.

Für allfällige Fragen stehe ich gern zur Verfügung.

Mit vorzüglicher Hochachtung

Dr. Hans G. Zeger, Obmann ARGE DATEN

PS: Ich behalte mir vor diesen Brief und Ihre geschätzte Anwort der interessierten Öffentlichkeit, jedenfalls den betroffenen Personen zur Verfügung zu stellen.

PPS: Selbstverständlich gilt für genannte Personen und Einrichtungen die Unschuldsvermutung.

Unser Werdegang

1995 Deltavista wurde zuerst unter dem Namen IQA mit der primären Aufgabe gegründet, eine Plattform für den Austausch von Adressbezogenen Daten zu bauen.

1998 Die Plattform "OK-Online" mit dem Fokus auf Risikomanagement wird produktiv gesetzt.

2000 Gründung der österreichischen Niederlassung in Wien.
Deltavista wächst auf 16 Mitarbeiter.

2001 Gründung der polnischen Niederlassung in Krakau.
Gründung der deutschen Niederlassung in München.
Der Firmenname wird von IQA auf Deltavista geändert.
Deltavista wächst auf 32 Mitarbeiter.

2002 Deltavista wächst auf 85 Mitarbeiter, davon sind 65 hoch qualifizierte Software-Ingenieure.

2003 OK-Online wird in ***Deltavista Online*** umgenannt, mit zusätzlichen Funktionalitäten und einem neuen Design versehen, was den Bedienungskomfort weiter verbessert.
Produktivsetzung des ersten Inhouse-Systems für Compliance (AML) bei einer führenden Schweizer Bank.
Deltavista wächst auf über 110 Mitarbeiter, davon sind 85 sehr qualifizierte Software-Ingenieure.

2004 Das zweite Inhouse-System für Risiko-Management wird bei einem grossen Schweizer Kreditkarten-Verarbeiter eingeführt
Die Aktionärsstruktur wird bereinigt und eine neue, fokussierte Datenstrategie ausgearbeitet: "Daten sammeln - Daten verarbeiten - Daten verkaufen"

2005 Die 2004 formulierte Strategie wird mit folgenden Massnahmen umgesetzt.

- das Management Team wird in allen Ländern mit erfahrenen Führungskräften verstärkt
- vier marktführende Daten produzierende Unternehmen werden übernommen oder eingebunden (KreditInform und Infodata in Österreich, InFoScore Zoom und InFoScore Cresura in der Schweiz)
- die Datenpflegeteams werden von 10 auf 20 Mitarbeiter ausgebaut

Das Umsatzwachstum von 60% über alle Länder hinweg bestätigt den Erfolg der Strategie

2006 Die erfolgreiche Strategieumsetzung wird weitergeführt

- in allen Ländern werden Anzahl und Qualität der Datenlieferanten erhöht
- Der Bedarf der Kunden an Daten und deren Interpretation wird mit einer Serie von neuen Produkten gedeckt
- Mit branchenspezifischen Poolinglösungen wird das Risikomanagmentangebot ausgeweitet.
- die Kooperation mit Informa, dem marktführenden Anbieter von Scoringdienstleistungen im deutschspachigen Raum, unterstützt die Entwicklung von neuen, hochwertigen Scoring-Produkten.

Benötigen Sie Hilfe?
tel.: +41 848 333 222
support@deltavista.com

Login für "Deltavista Online"

Land CH
Name
Passwort »

Last update: 24.10.2006

Geschäftsbedingungen

1. Der Besteller bestätigt, an den Mitteilungen der "Kreditinformationen" ein berechtigtes Interesse zu haben, da Informationen über (auch zwischenzeitig beendete) Exekutions- und Insolvenzverfahren seiner potentiellen Vertragspartner und Kunden in seine künftigen Entscheidungen einbezogen werden.
2. Der Besteller nimmt zur Kenntnis, daß die Mitteilungen in der "Kreditinformationen" nicht öffentlich erfolgen und streng vertraulich zu behandeln sind, somit ausschließlich für Überlegungen und Entscheidungen des Bestellers bestimmt sind und dieser jede Weitergabe einer Mitteilung oder Teilen hieraus zu unterlassen hat.
   Bei Zuwiderhandeln des Bestellers hat dieser für jedweden dadurch verursachten Schaden aufzukommen.
3. Der Besteller nimmt zur Kenntnis, daß die Mitteilungen in den "Kreditinformationen" auf verschiedensten Informations-Quellen basieren, die Daten sich auf den Erhebungszeitraum beziehen und Einstellungen von Exekutions- bzw. Insolvenzverfahren nicht überprüft werden und dies somit auch nicht zu Korrekturen in Datenträgern, Internet usw. und auch nicht zu einer Mitteilung in späteren Ausgaben führt.
4. Als Erfüllungs- und Gerichtsstand wird Wien vereinbart.

JUSTIZ BUNDESMINISTERIUM FÜR JUSTIZ

Museumstraße 7
1070 Wien

Tel.: +43 1 52152 2179
E-Mail: team.pr@bmj.gv.at

Sachbearbeiter/in:
Mag. Thomas Köberl

P.P.11

Dr. Hans G. Zeger
ARGE DATEN
Österreichische Gesellschaft für Datenschutz
Redtenbachergasse 20
1160 Wien

EINGEGANGEN
22. Sep. 2011
RSCHT11 3P1

Betrifft: Rechtswidrige Abfragen/Verwendung von Exekutionsdaten; Stellungnahme des Bundesministeriums für Justiz

Sehr geehrter Hr. Dr. Zeger,

ich darf Ihnen die Stellungnahme des Justizressorts zu den von der ARGE DATEN übermittelten Fragen zukommen lassen, wobei ich vorweg um Verständnis ersuche, dass ein in diesem Zusammenhang nach wie vor anhängiges strafrechtliches Ermittlungsverfahren bei der Zentralen Staatsanwaltschaft zur Verfolgung von Korruption in Wien sowie sicherheitstechnische Erwägungen eine Einschränkung des Auskunftsumfangs gebieten.

Ich verweise darüber hinaus auf die beiden parlamentarischen Anfragebeantwortungen

„Datenmissbrauch mit gerichtlichen Exekutionsdaten“ (7674/AB) und

"Exekutionsdaten - Korruption in der österreichischen Justiz?" (7840/AB),

mit denen die Bundesministerinnen für Justiz Mag. Bandion-Ortner und Dr. Beatrix Karl zum gleichen Komplex bereits Stellung genommen haben. Die darin enthaltenen Informationen sind nach wie vor aktuell. Sie sind diesem Schreiben zu Ihrer Kenntnisnahme angeschlossen. Darüber hinaus haben Experten des Bundesministeriums für Justiz in der Zwischenzeit dem Datenschutzrat Rede und Antwort gestanden.

Ich nehme die Gelegenheit schließlich wahr, für das konstruktive Gespräch vom 6. Mai 2011 und die grundsätzliche Bereitschaft der ARGE DATEN zu danken, das Bundesministerium für Justiz bei der Bewältigung und Aufarbeitung des Datenmissbrauchs zu unterstützen und zu beraten. Für die eingetretene Verzögerung bei der Beantwortung der Fragen wird um Nachsicht gebeten.

Zu den Fragen im Einzelnen:

Zu 1 bis 3:

Bei der Zentralen Staatsanwaltschaft zur Bekämpfung von Korruption ist ein strafprozessuales Ermittlungsverfahren anhängig, das den von der ARGE DATEN relevierten Datenmissbrauch zum Gegenstand hat. Nach der Verdachtslage haben Justizmitarbeiter systematisch bis zum 20. Oktober 2010 Daten aus dem elektronischen Exekutionsregister der Verfahrensautomation Justiz (VJ) ausgedruckt und gegen Entgelt an J. H. als Inhaber der in Wien ansässigen Firma K. weitergegeben.

Nach Eingabe in eine Datenbank der Firma K. wurden die Ausdrucke vernichtet. Daher ist der genaue Umfang der Datenweitergabe nur mit erheblichen Schwierigkeiten feststellbar. Diese Daten – deren Herkunft sodann nicht mehr erkennbar war – wurden in der Folge exklusiv an die ebenfalls in Wien ansässige Firma D. GmbH verkauft.

Die Datenbank der Firma K. wurde – vor ihrer Löschung auf den Servern der Firma K. – als Beweismittel sichergestellt. Die von J. H. bzw. der – nicht mehr existierenden – Firma K. angelegte Datenbank wurde unwiederbringlich gelöscht und ist damit jeglicher weiteren missbräuchlichen Verwendung entzogen.

Nach den dem Bundesministerium für Justiz vorliegenden Informationen wurde der von der Firma D. GmbH mit J. H. abgeschlossene Datenübermittlungsvertrag unmittelbar nach Festnahme des J. H. gekündigt und seitens der Rechtsvertretung des J. H. der Firma D. GmbH die Weiterverwendung der Daten untersagt. Im Zusammenhang mit der Erlassung einer einstweiligen Verfügung gegen die Firma D. GmbH wies diese darauf hin, dass sie „unverzüglich, bei erstmaligem Bekanntwerden fundierter Bedenken gegen die von der Firma K. geübte Praxis der Datenermittlung alle als Verwendung zu Wettbewerbszwecken in Betracht kommenden Applikationen der von der Firma K. stammenden Daten eingestellt habe".

Die Erhebungen zur Anzahl der betroffenen Personen sind noch im Gang.

Das Bundesministerium für Justiz ist nunmehr bestrebt den Betroffenen alle Informationen gemäß § 24 Abs 2a DSG zukommen zu lassen, um diesen die Wahrnehmung ihrer Datenschutzrechte zu ermöglichen. Eine solche Information der Betroffenen war bislang nicht möglich, weil nach dem derzeitigen Stand der Ermittlungen noch nicht bekannt ist, wie viele und welche Personen von den derzeit zu untersuchenden Vorgängen betroffen und welche Daten rechtswidrig weitergeleitet worden sind.

Es wird jedenfalls eine Form der Information angestrebt, die (zumindest) den Großteil der als betroffenen Identifizierten verlässlich erreicht. Diese sollen bei der Aufklärung ihrer Rechte

unterstützt werden und über geeignete Anlaufstellen die Möglichkeit erhalten, Anfragen an das Bundesministerium für Justiz zu richten.

Zu 4 bis 6:

Eine direkte Unterstützung von einzelnen Betroffenen im Verfahren zur Durchsetzung von Löschungs- oder Schadenersatzansprüchen durch das Bundesministerium für Justiz wäre im Rahmen des Zivilverfahrensrechts nur dann möglich und zulässig, wenn das Bundesministerium für Justiz ein rechtliches Interesse am Obsiegen der Betroffenen in den jeweiligen Verfahren hätte und daher eine gesetzliche Grundlage für eine Nebenintervention als Streithelfer auf ihrer Seite bestünde. Soweit ersichtlich besteht ein derartiges rechtliches Interesse jedoch nicht.

Eine indirekte – finanzielle – Unterstützung von einzelnen Betroffenen im Verfahren zur Durchsetzung von Löschungs- oder Schadenersatzansprüchen durch das Bundesministerium für Justiz käme nur dann in Betracht, wenn das Bundesministerium für Justiz dafür eine allgemeine gesetzliche Grundlage und ein entsprechendes Budget hätte („Förderung der Durchsetzung der Rechtsordnung im Einzelfall"), dazu im konkreten Fall aus Gründen der Amtshaftung verpflichtet wäre („Beistandspflicht zur Naturalrestitution") oder dies als geeignete Form der Leistung von Schadenersatz betrachten würde („Bereitstellung eines Deckungsfonds vorweg"). Ersteres ist soweit ersichtlich nicht der Fall, auch Zweiteres kann generell ausgeschlossen werden, weil selbst eine allfällige Amtshaftung stets auf Geld gerichtet ist (§ 1 Abs. 1 AHG: „Der Schaden ist nur in Geld zu ersetzen."). Der Frage „Bereitstellung eines Deckungsfonds vorweg" könnte nur für den Fall näher getreten werden, dass tatsächlich eine Haftung des Bundesministeriums für Justiz im Raum stünde.

Im Bundesvoranschlag 2011 sind grundsätzlich (und das ist auch für die nächsten Jahre so vorgesehen) 1,2 Mio. Euro für Schadenersatzzahlungen, insbesondere nach dem AHG, budgetiert.

Zu 7:

In dem genannten Verfahren hat die Staatsanwaltschaft Wien die Ermittlungen am 2. Juni 2008 im Wesentlichen mit der Begründung eingestellt, dass die Weitergabe der Daten im Rahmen der vom Beschuldigten gewerberechtlich genehmigten Auskunftei erfolgt sei und darüber hinaus Verjährung vorgelegen habe.

Im Lichte der neu zu Tage getretenen Vorwürfe und aktuellen Ermittlungsergebnisse wird allenfalls eine Verfahrensfortführung zu prüfen sein.

Zu 8 bis 10:

Die einschlägigen justizinternen Bestimmungen sehen vor, dass jeder Zugriff auf Registerdaten ausschließlich im Rahmen dienstlicher Notwendigkeiten zulässig ist. Sämtliche Zugriffe – sowohl lesend als auch bearbeitend – wurden und werden im Sinne der Bestimmung des § 14 Abs. 2 Z 7 DSG 2000 lückenlos protokolliert. Diese Informationen über Art und Zeitpunkt der erfolgten Zugriffe erweisen sich auch im Rahmen des laufenden Strafverfahrens als wertvoller Behelf zur Klärung der Faktenlage.

Zu 11 und 12:

Bereits nach Bekanntwerden der ersten Verdachtsfälle wurden einschränkende Maßnahmen getroffen, die ein unbefugtes Zugreifen von Benutzern verhindern. Darüber hinaus wurden technische Veranlassungen getroffen, die eine weitere Einschränkung der Möglichkeiten zur Namensabfrage bewirken. Qualifizierte Namensabfragen müssen nunmehr mit einer kurzen Begründung versehen werden. Geplant ist, in Hinkunft nach dem Zufallsprinzip ausgewählte Stichproben von Datenzugriffen auf ihre Rechtmäßigkeit zu überprüfen.

Maßnahmen zur Prävention von Datenmissbrauch durch Verhinderung unerlaubter Registerabfragen und Sensibilisierung der Mitarbeiter werden auch im Bereich der Dienstaufsicht und der Inneren Revision, so etwa zuletzt im Rahmen eines Workshops am Oberlandesgericht Linz, überlegt.

In Schulungsveranstaltungen und über Intraneteinschaltungen wird auf die engen Grenzen, innerhalb derer ein Zugriff auf Justizdaten zulässig ist, sowie auf die zu gewärtigenden, straf- und disziplinarrechtlichen Folgen bei Verstößen mit Nachdruck hingewiesen.

Zu 13 und 14:

Die Justiz bedient sich zur Erfüllung ihrer Aufgaben im Informationstechnologie-Bereich weitgehend der Bundesrechenzentrum GmbH, deren Sicherheitsstandards in Berücksichtigung ihrer Verantwortung für einen umfangreichen Bestand an höchst sensiblen Verwaltungsdaten entsprechend hoch angelegt sind. Der Schutz der Vertraulichkeit und Integrität und die Sicherstellung der Verfügbarkeit der Daten stellen die zentrale Aufgabe für die Sicherheitsmannschaft der Bundesrechenzentrum GmbH dar. Dazu wurde ein Managementsystem für Informationssicherheit eingerichtet, das die Vorgaben der ISO Norm 27001/ISO 17799:2005 erfüllt. Die Sicherheit der Informationen wird durch ein unabhängiges Gutachten geprüft und durch eine jährliche Zertifizierung bestätigt.

Im Jahr 2005 hat das Bundesministerium für Justiz die Bundesrechenzentrum GmbH mit der Durchführung eines „Vulnerability Scans“, der Errichtung eines „Intrusion Detection Systems“ und der Mitarbeit bei der Erstellung einer Arbeitsplatz-Sicherheits-Policy beauftragt. Letzteres

hat zur Ausarbeitung und Verbreitung von Merkblättern für Internet am Arbeitsplatz, die E-Mail-Nutzung und die IT-Sicherheit am Arbeitsplatz geführt. Im Jahr 2006 wurde ein Merkblatt für den Einsatz von Notebooks (Laptops), 2007 eine Regelung für das sichere Löschen von Festplatten und 2009 ein Merkblatt für die Verwendung von dienstlichen Mobiltelefonen verteilt. Diese Merkblätter werden aktuell gehalten und ihr Inhalt wird von den IT-Schulungszentren aktiv vermittelt. Ihre jeweils aktuelle Fassung wird auch im Intranet der Justiz bereit gestellt.

Die Empfehlungen des Österreichisches Informationssicherheitshandbuchs werden dabei nach Maßgabe der personellen und finanziellen Ressourcen berücksichtigt.

Wien, 19. September 2011
Für die Bundesministerin:
Dr. Josef Bosina

Elektronisch gefertigt