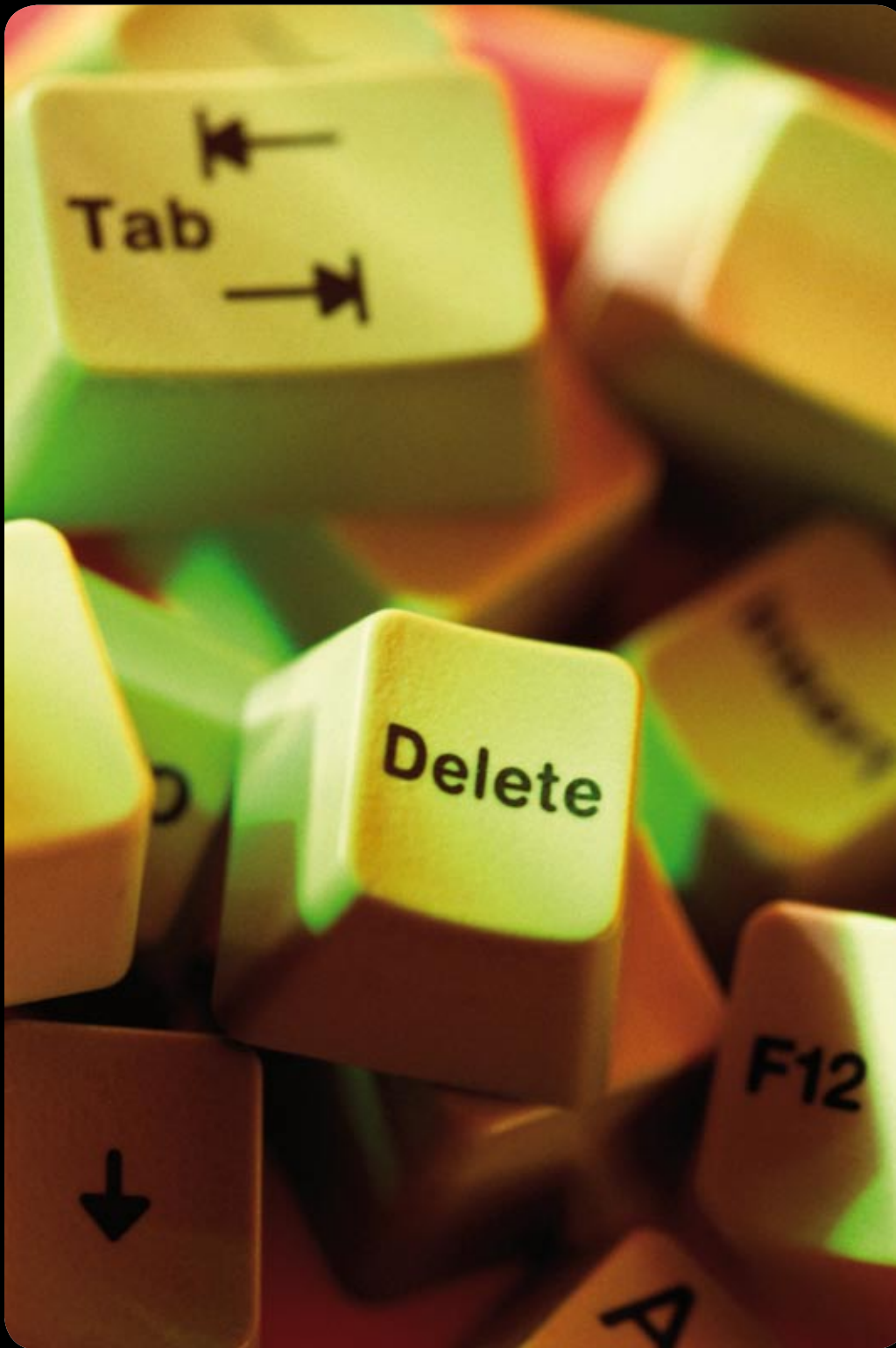


Datenschutz news**box**



Ausgabe

3

03/2010

Wie sicher ist der „sichere Hafen“?	2
Bundesverfassungsgericht stoppt Vorratsdatenspeicherung.....	3
EU-Kommission aktualisiert Standardvertragsklauseln	3
Chaos Computer Club fordert Einführung eines Datenbriefs	4
Weitergabe von Patientenangaben an private Abrechnungsstellen soll weiter möglich bleiben	4
Erpressung mit Sozialdaten bei der BKK Gesundheit	5
500.000 EUR Bußgelder wegen unerlaubter Telefonwerbung.....	5
Datenschutz auf Reisen wird von Unternehmen vernachlässigt.....	6
Jährliche kostenfreie Schufa-Auskunft.....	6
Gendiagnostikgesetz tritt in Kraft	6
Datenstriptease oder auch Blippy	7
EU-Datenschutzgesetze veraltet?	7
3. GDD-Fachtagung „Datenschutz International“	7
GDD startet Benchmarking zum Datenschutz	8



Editorial:

Der 1. April 2010... Da ist doch noch was?

Waren Sie seit dem 1. September 2009 auch damit beschäftigt Ihre „Altverträge“ mit Dienstleistern aus dem Bereich der Auftragsdatenverarbeitung auf den aktuellen Stand des § 11 BDSG zu bringen? Oder haben Sie vielleicht Wochen damit verbracht ein neues „Incidentmanagement“ auf die Beine zu stellen, welches auch den § 42a BDSG berücksichtigt? Möglicherweise haben Sie sich aber auch den Kopf darüber zerbrochen, ob die Unternehmens-Compliance nicht doch auf wackeligen Beinen steht, nach Inkrafttreten des neuen § 32 BDSG?

Fest steht, dass Sie als Datenschutzbeauftragter, insbesondere in den letzten Monaten gut beschäftigt gewesen sein müssen.

Und trotzdem: Sie sollten nicht vergessen, dass zum 1. April 2010 noch was kommt..., empfiehlt Ihnen Ihr

RA Levent Ferik,
Gesellschaft für
Datenschutz und Datensicherheit

Wie sicher ist der „sichere Hafen“?

Nach einem Bericht von heise-online soll das sog. Safe-Harbor-Abkommen einer kritischen Prüfung unterzogen werden.

Safe Harbor ist eine besondere Datenschutz-Vereinbarung zwischen der Europäischen Union und den Vereinigten Staaten, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln.

Die Richtlinie 95/46/EG (Datenschutzrichtlinie) verbietet es grundsätzlich, personenbezogene Daten aus EG-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da diese keine umfassenden gesetzlichen Regelungen kennen, die den Standards der EU entsprechen.

Damit der Datenverkehr zwischen den USA und der EU nicht zum Erliegen kommt, wurde zwischen 1998 und 2000 ein besonderes Verfahren entwickelt. US-Unternehmen können dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die Safe Harbor Principles (englisch für „Grundsätze des sicheren Hafens“) und die dazugehörigen – verbindlichen – Frequently Asked Questions (FAQ) zu beachten. Im Jahr 2000 hat die EU anerkannt, dass bei den Unternehmen, die dem Safe-Harbor-System beigetreten sind, ein ausreichender Schutz besteht.

Die Anregung zur Prüfung dieses Verfahrens kommt vom sog. Düsseldorfer Kreis, dem die deutschen Datenschutz-Aufsichtsbehörden angehören. Dieser wird Ende April eine entsprechende Entschließung diskutieren.

Mit ein Grund für die kritische Betrachtung des Abkommens sei ein Gutachten des US-Beratungsunternehmens Galexia. So habe die Studie z.B. zu Tage gefördert, dass 206 Unternehmen, die behaupteten Mitglied von Safe Harbor zu sein, gar keine Mitglieder waren. Kritisch betrachtet wird auch die Tatsache, dass die Sanktionswirkung für solche Falschangaben wohl eher gering sein wird, da nur ein einziges Unternehmen wegen dieser wahrheitswidrigen Angaben in den USA verurteilt worden sei. Daher befürchtet der schleswig-holsteinische Landesdatenschützer Thilo Weichert, dass „das Safe-Harbor-Abkommen zu einer Art Freibrief für die Amerikaner geworden sei“ und Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sieht die Aussagekraft des Abkommens als sehr kritisch.

Quelle: heise.de

Bundesverfassungsgericht stoppt Vorratsdatenspeicherung

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht die Nichtigkeit der bislang bestehenden Regelungen zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten festgestellt. Zwar sei die Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehle aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisteten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten.

Das Bundesverfassungsgericht ist der Auffassung, dass die Anforderungen an die Verwendung der gespeicherten Vorratsdaten nicht den bestehenden verfassungsrechtlichen Anforderungen

genügen. Insbesondere sei es für den Zugriff auf die Daten alleine nicht ausreichend, dass die verfolgte Straftat mittels Telekommunikation begangen worden sei. Erforderlich für den Abruf der Daten sei vielmehr, dass der begründete Verdacht für eine auch im Einzelfall schwerwiegende Straftat bestehe. Für eine verfassungskonforme Ausgestaltung der Vorratsdatenspeicherung fordert das Bundesverfassungsgericht außerdem, dass für bestimmte auf besondere Vertraulichkeit angewiesene Telekommunikationsverbindungen (z.B. im Bereich der Sozialberatung) ein grundsätzliches Übermittlungsverbot vorgesehen wird.

Quelle: Pressemeldung der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

EU-Kommission aktualisiert Standardvertragsklauseln

Die Europäische Kommission hat am 5.2.2010 die so genannten „Standardvertragsklauseln“ aktualisiert. Am 15. Mai 2010 treten die bisher gültigen Standardklauseln außer Kraft. Relevanz hat diese Aktualisierung für alle verantwortlichen Stellen, soweit sie Lieferanten, Kunden oder Konzerngesellschaften außerhalb der EU personenbezogene Daten zur Verfügung stellen.

Vizepräsident Jacques Barrot erklärte hierzu: „ Die Standardvertragsklauseln wurden geändert, um neuen Geschäftsmodellen sowie der zunehmenden Globalisierung und Auslagerung von Da-

tenverarbeitungstätigkeiten Rechnung zu tragen. Somit finden die Anforderungen des internationalen Handels und der Schutz personenbezogener Daten von EU-Bürgern ausgewogen Berücksichtigung.“

Damit werde unter anderem der Ausweitung von Datenverarbeitungstätigkeiten und neuen Geschäftsmodellen für die internationale Verarbeitung personenbezogener Daten Rechnung getragen.

Quelle: Pressemeldung Portal der Europäischen Union

Chaos Computer Club fordert Einführung eines Datenbriefs

Der Chaos Computer Club fordert zur Stärkung des Rechts auf informationelle Selbstbestimmung die Einführung eines sog. Datenbriefs. Danach soll jede speichernde Stelle (öffentlich und nicht-öffentlich) verpflichtet sein, den Bürger von sich aus regelmäßig über die gespeicherten personenbezogenen Daten zu informieren. Einmal pro Jahr soll darüber informiert werden, welche persönlichen Daten wo gespeichert sind.

Ganz neu ist diese Idee des Chaos Computer Clubs nicht. Neu ist jedoch, dass dies in Zeiten immer wieder auftretender Datenschutzskandale und gesteigerter Datenschutzsensibilität offen, kontrovers und ernsthaft diskutiert wird. Befürworter eines solchen Datenbriefs müssen sich zumindest die Fragen gefallen lassen, ob die Verbraucher die nicht angeforderte Post wollen und ob damit nicht wieder ein bürokratisches „Datenmonster“ geschaffen würde sowie die Frage, ob das gesetzlich bereits verbriefte Auskunftsrecht nicht schon ausreichend ist?

Quelle: [Internetseite Chaos Computer Club](#) und [Taz.de](#)

Weitergabe von Patientenangaben an private Abrechnungsstellen soll weiter möglich bleiben

Nach einer Entscheidung des Bundessozialgerichts Ende 2008 (Aktenzeichen: B 6 KA 37/07 R, BSG 6. Senat), sollte die Weitergabe von Patientendaten durch Krankenhäuser oder Vertragsärzte an private Dienstleistungsunternehmen zur Erstellung von Abrechnungen nicht mehr zulässig sein. Eine Legitimierung dieser Verfahrensweise, selbst im Wege der Abgabe von Einwilligungserklärungen durch den Betroffenen wurde vom Bundessozialgericht ausgeschlossen. Das Gericht begründet dies mit dem besonderen Schutz der sehr sensiblen personenbezogenen Gesundheitsdaten. Nach dem für die gesetzliche Krankenversicherung geltenden Sozialgesetzbuch dürfen eigentlich nur die Krankenkassen und die Kassenärztlichen Vereinigungen mit den Daten der Patienten arbeiten. Sie unterliegen im Unterschied zu privaten Anbietern den strengen Datenschutzregeln des Sozialrechtes. Aufgrund der Tragweite und Konsequenz des Bundessozialgerichts-Urteils ließ sich eine kurzfristige Änderung der Abrechnungspraxis nicht umsetzen, so dass es nach einem Erlass der damaligen Regierung bis Mitte 2010 durch eine Ausnahmeregelung die Verfolgung der bisherigen Abrechnungspraxis möglich sein sollte. Diese Ausnahmeregelung stieß schon damals auf Ablehnung des Bundesdatenschutzbeauftragten Schaar, so dass als Kompromiss die umfassende gesetzliche Neuregelung der Abrechnungspraxis in den Raum gestellt wurde.

Nun möchte Gesundheitsminister Rösler eine weitere Verlängerung der Ausnahmeregelung bis 30. Juni 2011. Von diesem Verfahren sind Millionen Versicherte betroffen und die Frage stellt sich, ob bei einer Weitergabe an private Dienstleister der Schutz der relevanten Gesundheitsdaten gewährleistet ist. Dass diese Frage ihre Berechtigung hat und was passieren kann, wenn hochsensible medizinische Daten von Versicherten in die Hände von Unbefugten gelangen, macht auch die nachstehende Meldung deutlich.

Quelle: [Internetseite Berliner Zeitung](#)

Erpressung mit Sozialdaten bei der BKK Gesundheit

Wenn man bei der Frage, ob sich der Ankauf einer „Steuersünder-CD“ moralisch wie strafrechtlich vertreten lässt – wie auch die öffentlichen Diskussionen der letzten Wochen zeigen – noch gespaltener Meinung sein kann, ist dieser Fall moralisch wie strafrechtlich eindeutig.

Was bei einer Einschaltung privater Unternehmen mit Patientendaten passieren kann, zeigt ein Vorfall bei der Krankenkasse BKK Gesundheit, die im Januar 2010 von einem Unbekannten erpresst wurde. Ein Mann hatte der größten deutschen Be-

triebskrankenkasse BKK Gesundheit Unterlagen von BKK-Kunden zum Kauf angeboten. Zugleich drohte er damit, die Daten zu veröffentlichen, sollte die Kasse nicht darauf eingehen.

Das Datenleck hatte seine Entstehung anscheinend darin, dass die Krankenkasse eine externe Firma mit der Betreuung ihrer Telefon-Hotline betraut hatte. Diese wiederum beschäftigte einen Subunternehmer, der Hilfskräfte beauftragte. Den Hilfskräften sei es möglich gewesen von privaten Computern oder Laptops medizinische Diagnosen und andere Daten abzurufen und speichern zu können.

Einer der Mitarbeiter war den Angaben der Krankenkasse zufolge wahrscheinlich in den Besitz der Kundendaten gekommen, die zum Beispiel medizinische Diagnosen enthielten. Damit wollte er die Krankenkasse dann erpressen. Die BKK Gesundheit erstattete jedoch Anzeige.

Nach Angaben der BKK Gesundheit sei nach dem Vorfall der Zugang zu Kundendaten für alle externen Dienstleister sofort abgeschaltet und sämtliche Zugangskennungen gesperrt worden. Auch habe man alle zuständigen Aufsichtsbehörden umfassend informiert.

Quelle: Sueddeutsche.de

500.000 EUR Bußgelder wegen unerlaubter Telefonwerbung

Die Bundesnetzagentur zieht Callcenter und ihre Auftraggeber wegen unerlaubter Telefonwerbung zur Rechenschaft. Im Dezember 2009 und Januar 2010 habe der Regulierer in neun Verfahren Bußgelder in einer Gesamthöhe von 500.000 Euro verhängt, teilte die Behörde in ihrer Pressemeldung mit.

Die Bundesnetzagentur ahndet damit erstmals Verstöße gegen das Verbot der unerlaubten Telefonwerbung und die Missachtung der Rufnummernanzeigepflicht bei Werbeanrufen.

Seit Inkrafttreten der Änderungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) und des Telekommunikationsgesetzes (TKG) am 4. August 2009 gelten Werbeanrufe ohne Einwilligung des Angerufenen und Werbeanrufe mit unterdrückter Rufnummer als Ordnungswidrigkeiten. Die nun auferlegten Bußgelder wurden sowohl gegen die Auftraggeber der Werbeanrufe als auch gegen die ausführenden Callcenter verhängt. In einer weiteren Bußgeldsache wurde das Verfahren aus Mangel an Beweisen eingestellt.

Die mit Bußgeldern belegten Unternehmen hatten in den konkreten Fällen unerlaubte telefonische Werbeaktionen ohne die ausdrückliche Einwilligung der Angerufenen durchgeführt oder Callcenter mit der Durchführung der Werbeanrufe beauftragt. Betroffen waren dabei unterschiedlichste Dienstleistungen und Produkte aus den Branchen Telekommunikation, Medien und Lotteriegewinne. Bei Verstößen gegen das Verbot der unerlaubten Telefonwerbung kann die Bundesnetzagentur nach dem UWG Bußgelder bis zu 50.000 Euro verhängen. Den gegenwärtigen Bußgeldbescheiden waren langwierige Ermittlungsarbeiten vorausgegangen.

Bußgeldrelevant war zudem auch die Rufnummernunterdrückung bei Werbeanrufen. In diesem Zusammenhang wurden Fälle mit Bußgeldern geahndet, in denen die Rufnummer des anrufenden Callcenters nicht angezeigt wurde oder das werbende Unternehmen eine ihm nicht zugeteilte Rufnummer hat anzeigen lassen. Die Falschanzeige verschleiern ebenso wie die Nichtanzeige der Rufnummer die Identität des Anrufenden. Bei Werbeanrufen mit unterdrückter Rufnummer kann die Bundesnetzagentur Bußgelder bis zu 10.000 Euro verhängen.

Quelle: Pressemitteilung Bundesnetzagentur

Datenschutz auf Reisen wird von Unternehmen vernachlässigt

Nur in knapp 60 Prozent der deutschen Unternehmen existiert ein Risikomanagement für Geschäftsreisen, das die spezifischen Risiken, die mit Geschäftsreisen verbunden sind, aktiv managt. Nur jedes dritte Unternehmen bindet das Risikomanagement für Geschäftsreisen in das generelle Risikomanagement der Unternehmen ein; in jedem fünften Unternehmen handelt es sich um ein eigenständiges System ohne Integration. Dies ergab eine Umfrage unter den im Verband Deutsches Reisemanagement e.V. (VDR) organisierten Travel Managern.

„Die Befragung macht deutlich, dass mit Geschäftsreisen vielfältige Risiken verbunden sein können, diese Risiken sich

aber nur in einzelnen Fällen im Risikobewusstsein niederschlagen. Das Risikomanagement für Geschäftsreisen ist zwar auf dem Vormarsch, sollte jedoch weiter ausgebaut und insbesondere auch besser in das allgemeine Risikomanagement der Unternehmen integriert werden“, fasst Thiesing das Umfrageergebnis zusammen.

Ebenfalls mit diesem Thema ist die Gewährleistung des technisch-organisatorischen Datenschutzes im Rahmen von z.B. Geschäftsreisen verknüpft. Denn nicht nur innerhalb der Räumlichkeiten einer Institution müssen Informationen angemessen geschützt werden, dies ist natürlich

auch außerhalb erforderlich. Mitarbeiter müssen mit sensiblen Informationen auch auf Geschäfts- oder Privatreisen sorgfältig umgehen. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich zum Thema Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung Gedanken gemacht und stellt diese auf seiner [Internetseite](#) zur Verfügung.

DATAKONTEXT bietet ein Merkblatt für Mitarbeiter „Unterwegs mit dem Notebook – aber sicher!“ an. Weitere Informationen finden Sie auf der [Homepage](#).

Quellen: [Pressemeldungen Osfalia](#) und [Verband Deutsches Reisemanagement](#)

Jährliche kostenfreie Schufa-Auskunft

Die Kreditauskunft Schufa hat verbesserte Auskunftsmöglichkeiten vorgestellt. Verbraucher können demnach ab dem 1. April einmal im Jahr für sie kostenfrei Einblick in die über sie gespeicherten Daten bei der Kreditauskunft Schufa verlangen. Ermöglicht wird dies durch eine Änderung des Bundesdatenschutzgesetzes, das im Frühjahr 2009 von Bundestag und Bundesrat beschlossen worden war. Bei diesen Neuerungen geht es vor allem um den Zugang von Verbrauchern zu ihren gespeicherten Informationen und eine umfassendere Erläuterung der Informationen.

„Wir begrüßen die Entscheidung des Gesetzgebers für mehr Transparenz bei Auskunfteien. Es ist uns sehr wichtig, Verbrauchern einen Einblick in ihre gespeicherten Informationen zu geben – dazu gehört nach unserem Verständnis aber nicht nur ein Erfüllen der gesetzlichen Mindestanforderungen wie das Angebot einer kostenlosen schriftlichen Auskunft pro Jahr, sondern weitaus mehr“, heißt es in der Presseerklärung der Schufa. Die Regelung gilt für alle Auskunfteien.

Quelle: [Pressemitteilung Schufa](#)

Gendiagnostikgesetz tritt in Kraft

Im Frühjahr 2009 hatten sich CDU/CSU und SPD nach jahrelangem Streit auf ein Gendiagnostikgesetz verständigt. Danach dürfen Arbeitgeber nur in Ausnahmen Gentests verlangen, Versicherungen Erbgut-Analysen nur in bestimmten Fällen einsehen dürfen. Das Gesetz, das Benachteiligungen aufgrund genetischer Eigenschaften verhindern soll, ist am 1. Februar 2010 in Kraft getreten.

Generell müssen laut dem rechtlichen Normenwerk Erwachsene in Gentests nach gründlicher Beratung ausdrücklich einwilligen. Ferner dürfen Betroffene über die Weitergabe, Aufbewahrung oder Vernichtung ihrer Gendaten bestimmen. Eine Ausnahme gilt für Versicherungen bei hohen Auszahlungssummen. Eine genetische Untersuchung zu medizinischen Zwecken darf laut dem Gesetz nur von einem Arzt vorgenommen werden. Erlaubt die Analyse eine Vorhersage über die eigene Gesundheit oder die eines ungeborenen Kindes, ist eine genetische Beratung verpflichtend. Wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, in einer Pressemeldung vermeldet, begrüßt er die zahlreichen datenschutzkonformen Regelungen, bedauert jedoch, dass das Gesetz keine Regelungen zum Umgang mit genetischen Untersuchungen im Zusammenhang mit Forschungen beinhaltet.

Quelle: [Pressemitteilung BfDI](#)

Datenstriptease oder auch Blippy

In Zeiten von Payback und diversen Social Networks glaubt man, dass der Gipfel der Selbstentblößung erreicht ist und nicht mehr viel Neues hinzu kommen kann, was den Grad des bedenkenlosen Umgangs mit den eigenen personenbezogenen Daten steigern könnte.

Man wird aber doch immer wieder eines Besseren belehrt und ahnt, dass nicht die Gegenwart den Zenit der freiwilligen Aufgabe über die Kontrolle der eigenen

Daten markiert, sondern oftmals die eigene Phantasie nur nicht ausreichend ist, um sich das vorzustellen, was wohl noch kommen mag. So stellt Blippy das dar, was sich einige sicher vor einigen Jahren noch nicht vorstellen konnten, jetzt aber als Dienst bereits läuft. Oder hätten Sie vor einigen Jahren gedacht, dass Verbraucher freiwillig ihre Kreditkarteninformationen auf der Webseite eines Unternehmens eintragen, sowie die Zugangsdaten

zu allen Websites, bei denen sie als Käufer registriert sind, etwa iTunes und Amazon, damit bei jedem Bezahlvorgang mit Ihrer Kreditkarte auf der Webseite eines Unternehmens veröffentlicht wird, was sie zu welchem Preis gekauft haben? Vorerst funktioniert Blippy in der Vollversion nur mit einer in den USA erworbenen Kreditkarte.

Quelle: [Zeit Online](#)

EU-Datenschutzgesetze veraltet?

Chef-Anwalt und Senior Vice President von Microsoft Brad Smith bewertet den Datenschutz innerhalb Europas als veraltet. Dies wurde in seinem Vortrag „Technology Leadership in the 21' Century“ deutlich, welches er Ende Januar im Museum of Art and History in Brüssel hielt.

Brad Smith Forderungen konzentrierten sich auf neue Gesetze für Datenschutz und Vorratsdatenspeicherung. Verbesserungsbedarf sieht Brad Smith insbesondere hinsichtlich der datenschutzrechtlichen Herausforderungen, die das sog. Cloud Computing mit sich bringe.

Diesen Herausforderungen könne nur begegnet werden, wenn Regelungen im Datenschutzrecht diesbezüglich angepasst würden. Derzeit seien die Gesetze auf einem Stand, der etwa Mitte der 1990er Jahre aktuell gewesen ist, so Smith.

Als hinderlich und suboptimal seien auch die unter den EU-Ländern noch nicht harmonisierten Regelungen zu bewerten, wobei Smith die Regelungen zur Vorratsdatenspeicherung hervorhob. Den gesamten Vortrag können Sie [hier](#) als Video abrufen.

Quelle: [silicon.de](#)

3. GDD-Fachtagung „Datenschutz International“ am 29. – 30. April 2010 in Berlin

Die 3. GDD-Fachtagung „Datenschutz International“ findet am 29. – 30. April 2010 in Berlin statt. Sie gewährt eine Übersicht und Diskussion aktueller Fragestellungen des internationalen Datenschutzes mit Experten des betrieblichen Datenschutzes und Vertretern der Aufsichtsbehörden sowie eine Vorstellung von Lösungsvorschlägen und Benchmarkmodellen.

Die Themen im Einzelnen (Auswahl):

- Die neue e-Privacy Directive
- Cloud Computing
- Die neuen EU Standardvertragsklauseln für Auftragsdatenverarbeiter
- „E-Discovery und Datenschutz – Erfahrungen aus der anwaltlichen Praxis“
- Paneeldiskussion - Evaluierung der EU-Datenschutz-Richtlinie
- Internationales Datenschutzaudit/Cert

Das vollständige Seminarprogramm finden Sie auf der [DATAKONTEXT-Homepage](#).

GDD startet Benchmarking zum Datenschutz

Die Organisation des Datenschutzes liegt in der Verantwortung von Unternehmen und Behörden. Bisher gibt es kaum aktuelle und aussagefähige Werte, wie diese ihren gesetzlichen Verpflichtungen zur Datenschutzorganisation nachkommen. Die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) möchte diese Lücke schließen. Dazu startet am 01.03.2010 das Privacy Panel.

Das Privacy Panel liefert eine umfassende und zeitnah aufbereitete Informationsbasis über die Situation des Datenschutzes in Unternehmen und Verwaltung. Die Auswertung erfolgt branchen- und größenbezogen.

Im GDD Privacy Panel werden die wesentlichen Themenfelder zur Umsetzung von Datenschutz, aber auch zu Aufgaben und Stellung des betrieblichen oder behördlichen Datenschutzbeauftragten betrachtet. In der geplanten jährlichen Befragung tragen alle Teilnehmer des Privacy Panels selber zur Aktualisierung der Benchmark-Datenbank bei. Dabei ermöglicht ein einheitliches Prozessmodell den Vergleich unterschiedlich aufgestellter Unternehmen.

Die Befragung zum GDD Privacy Panel erfolgt webbasiert. Die Auswertung der erhobenen Daten erfolgt weitgehend automatisiert. Die Ergebnisse bieten einen Vergleich zum Panel-Durchschnitt in den vom Teilnehmer beantworteten Fragen. Optional werden den Teilnehmern verschiedene Selektionsmöglichkeiten angeboten, mit denen sie den Vergleich hinsichtlich verschiedener Kriterien wie z.B. Unternehmensgröße oder Branchenzugehörigkeit individuell einschränken können. Folgende Mehrwerte können die Teilnehmer für sich in Anspruch nehmen:

- Ableitung von Tendaussagen auf Basis aktueller Daten
- Identifizierung von „Best Practices“
- Standortbestimmung bezüglich der eigenen Datenschutzorganisation
- Ggf. wichtige Kenndaten für die eigene Strategieentwicklung
- Argumentationskriterien gegenüber der Geschäftsleitung

Hier finden Sie weitere Informationen zum GDD Privacy Panel und eine Anleitung, wie Sie daran teilnehmen können.

[GDD Privacy Panel](#)

Die GDD bittet um eine rege Teilnahme am GDD Privacy Panel.

Quelle: [Gesellschaft für Datenschutz und Datensicherheit e.V.](#)