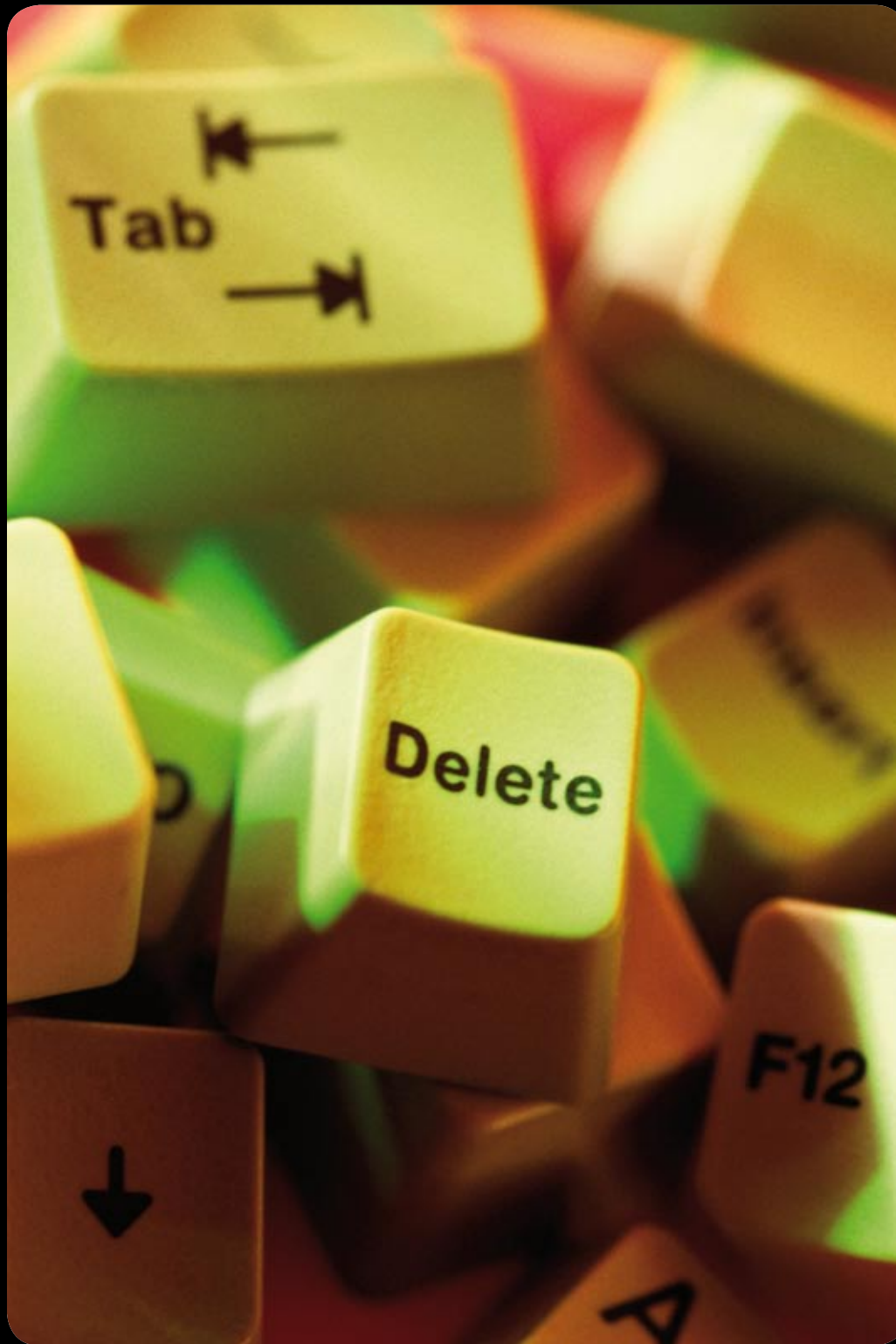


Datenschutz newsbox



Ausgabe

5

05/2009

Cloud-Computing mit BDSG vereinbar?	2
Datenschutzgesetze laufen ins Leere	3
Zähne für das Bundesdatenschutzgesetz	3
Arbeitnehmer-Foto auf Homepage auch nach Kündigung zulässig	3

Datenschutzfachtagung 2009 - Neues BDSG: Konsequenzen aus Datenschutzskandalen und Missmanagement	4
Fristlose Kündigung eines Systemadministrators wegen unerlaubtem Zugriff auf E-Mails	4

Der BGH zum Haftungsrisiko des Compliance Officers	5
Staatsanwaltschaft ermittelt gegen Kik	5
Google und Facebook müssen nachbessern	5
Staatliche Überwachung	6
Rechtsfolgen von Datenschutz-Pannen.....	6
Telekom erstattet Strafanzeige gegen Vertriebspartner	6
Stimmen zum Datenschutz bei der DB Sicherheit	6
Banken kontrollieren Daten beim Geldtausch	7
Verbraucherzentrale SH und ULD geben Infos zum illegalen Datenhandel	7
Neuregelung der Auftragsdatenverarbeitung nach §11 BDSG.....	7
„Projekt Datenschutz“ ist online	8
Fernmeldegeheimnis bedroht?	8
Wie man sich vor Datenmissbrauch schützen kann	8
Datenschutzskandal bei der Österreichischen Bundes- bahn (Sammeln von Krankenstandsdaten)	8



Editorial:

Beim Thema Cloud-Computing lässt sich oftmals feststellen, dass jeder seine eigene Vorstellung davon hat, um was es wohl gehen könnte. Was den Datenschutzbeauftragten ganz besonders interessiert: Um was handelt es sich dabei bei datenschutzrechtlicher Betrachtung?

Diese Frage versucht u.a. der kleine Exkurs zum Thema Cloud-Computing zu beantworten...

Jederzeit einen guten Durchblick wünscht Ihnen Ihr

Levent Ferik

Cloud-Computing mit BDSG vereinbar?

Die Frage der datenschutzrechtlichen Zulässigkeit von Cloud-Anwendungen wird oftmals kritisch betrachtet. Gernot Keckeis, Director Identity & Security Management, Novell DACH macht darauf aufmerksam, dass die Cloud-basierte Verarbeitung von Personendaten, die außerhalb der EU stattfindet laut dem deutschen Datenschutzrecht nicht zulässig sei. Das gehe aus dem aktuellen Jahresbericht des Berliner Datenschutzbeauftragten Alexander Dix hervor. Insbesondere, wenn es um den Schutz von sensiblen Daten gehe, sei es unumgänglich zu wissen, wo diese gespeichert werden und wer darauf zugreifen kann.

Aber um was genau handelt es sich bei Cloud Computing in datenschutzrechtlicher Hinsicht? Dazu ein Auszug aus dem besagten Tätigkeitsbericht von Herrn Dix:

Cloud Computing ist eine spezielle Ausprägung der Datenverarbeitung im Auftrag (§ 11 BDSG). Verarbeitet ein Auftragnehmer Daten für einen Auftraggeber, so gilt der Auftragnehmer nicht als Dritter im Sinne des Datenschutzrechts. Der Auftragnehmer trägt keine eigene Verantwortung für die Verarbeitung der Daten (mit Ausnahme seiner Verpflichtung zur Durchführung von technisch-organisatorischen Maßnahmen), der Auftraggeber bleibt datenschutzrechtlich verantwortlich für die Daten. Die Weitergabe der zu verarbeitenden Daten an den Auftragnehmer ist demzufolge keine Datenübermittlung, für die es eine Rechtsgrundlage geben müsste. Etwas anderes gilt jedoch, wenn der Auftragnehmer die Daten nicht innerhalb der EU bzw. des Europäischen Wirtschaftsraums verarbeitet. In diesem Fall ist er nach § 3 Abs. 8 Satz 3 Bundesdatenschutzgesetz (BDSG) Dritter, und die Bereitstellung der personenbezogenen Daten zum Zwecke der Auftragsdatenverarbeitung ist eine Übermittlung, deren Zulässigkeit sich an §§ 4b und 4c BDSG messen lassen muss. Cloud-Computing bietet Dienstleistungen mit personenbezogenen Daten, die völlig ortsunabhängig sind, also irgendwo in der Welt erbracht werden können, ohne dass die Kundin oder der Kunde wissen müsste, wo die Daten sind. Dies wäre aber nach den dargestellten datenschutzrechtlichen Ausnahmeregelungen für die Auftragsdatenverarbeitung in Drittstaaten nicht zulässig. Die datenschutzrechtlich für die Datenverarbeitung verantwortlichen, z. B. deutschen Kundinnen und Kunden, müssen sich davon überzeugen, dass die Datenverarbeitung nicht in einem Drittland ohne angemessenes Datenschutzniveau, z. B. in den USA, China oder Japan, stattfindet. Dies beschränkt die Ortsunabhängigkeit des Cloud-Computing. Aus diesem Grunde müssen die Cloud-Computing-Provider dem Beispiel Amazons folgen, die Dienstleistungen in unterschiedlichen Regionen mit gemeinsamen Datenschutzstandards anzubieten, also zum Beispiel innerhalb der EU und anderer Länder, die nicht als Drittländer anzusehen sind. Weitere wichtige Details und welche Anforderungen an ein datenschutzkonformes Cloud Computing zu stellen sind, können Sie dem aktuellen Tätigkeitsbericht des Berliner Beauftragten für den Datenschutz und Informationsfreiheit entnehmen (Seite 14 ff.).

Quellen: Silicon.de und Internetseite des Berliner Beauftragten für den Datenschutz und Informationsfreiheit

Beachten Sie in diese in diesem Zusammenhang auch die [Veröffentlichung eines Leitfadens](#) zum Thema Cloud-Computing durch den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM).



Impressum

DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort Frechen

Augustinusstraße 9d · 50226 Frechen
Tel.: 02234/966 10-0
Fax: 02234/966 10-9
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer: Clemens Köhler
Leitung: Hans-Günter Böse
Handelsregister
Mannheim HRB 337678

Datenschutzgesetze laufen ins Leere

Eine Studie des Karlsruher Instituts für Technologie lässt den großen Wirbel um die Novelle des Bundesdatenschutzgesetzes und die neuen Forderungen nach strengeren Gesetzen zum Schutze der personenbezogenen Daten von Kunden und Arbeitnehmern in einem ganz anderen Licht erscheinen.

Wissenschaftler des Karlsruher Instituts für Technologie (KIT) und der Universität Regensburg haben Dienste im Internet analysiert und massive Defizite aufgedeckt. Als Ergebnis konnte festgehalten werden, dass zwar meist hinreichende Datenschutzgesetze

existieren, die Schutzwirkung der Normen oft aber ins Leere läuft, da viele verantwortliche Stellen, sich nicht darum kümmern, dass sie eingehalten werden.

Den vollständigen Text der Pressemitteilung erhalten Sie als pdf-Dokument auf folgender Seite:
http://www.kit.edu/55_415.php

Quelle: Internetseite Karlsruhe Institute of Technology
<http://www.kit.edu/>

Zähne für das Bundesdatenschutzgesetz:

Petition zur Änderung des Bundesdatenschutzgesetzes

Seit dem 06.10.2009 ist eine E-Petition zur Änderung des Bundesdatenschutzgesetzes zur Mitzeichnung auf der Seite

<https://epetitionen.bundestag.de/index.php?action=petition;sa=details;petition=7180> freigeschaltet.

Der Initiator der Petition schlägt unter dem Motto „Zähne für das Bundesdatenschutzgesetz“ dort kleine Verbesserungen der Rechte der Betroffenen vor, damit das Recht auf Auskunft über die gespeicherten Daten auch praktisch durchsetzbar wird. Wird eine Petition innerhalb von 3 Wochen nach Eingang (bei öffentlichen Petitionen rechnet die Frist ab der Veröffentlichung im Internet) von 50.000 oder mehr Personen unterstützt, wird über sie im Regelfall im Petitionsausschuss öffentlich beraten. Der Petent wird zu dieser Beratung eingeladen und erhält Rederecht. Ausführlichere Erläuterungen zum Hintergrund der Petition erhalten Sie [hier](#).

Quelle: [Datenschutzforum des Bundesbeauftragte für den Datenschutz und die Informationsfreiheit](#)

Arbeitnehmer-Foto auf Homepage auch nach Kündigung zulässig

Nach einem aktuellen Beschluss des LAG Köln (Beschl. v. 10.07.2009 - Az.: 7 Ta 126/09) darf ein Foto, das am Arbeitsplatz aufgenommen wurde und eine Mitarbeiterin am Telefon zeigt, jedenfalls dann, wenn es keinen individualisierenden Bezug zu der Mitarbeiterin aufweist, auch nach Beendigung des Arbeitsverhältnisses weiter zu Illustrationszwecken auf der Homepage des Arbeitgebers verbleiben.

Ein während des Arbeitsverhältnisses zumindest stillschweigend erklärtes Einverständnis mit der Aufnahme erlösche nicht automatisch beim Ausscheiden aus dem Betrieb, sofern der Arbeitnehmer nicht ausdrücklich Gegenteiliges erklärt (hat).

Zumindest dann nicht, wenn das im Internet veröffentlichte Bild lediglich der allgemeinen Illustration diene und nicht auf die individuelle Person des Arbeitnehmers Bezug nehme.

Quelle: http://www.justiz.nrw.de/nrwe/arbgs/koelnllag_koelnlj2009/7_Ta_126_09beschluss20090710.html

Datenschutzfachtagung 2009 - Neues BDSG: Konsequenzen aus Datenschutzskandalen und Missmanagement

Die diesjährige DAFTA (Datenschutzfachtagung) wirft bereits ihre Schatten voraus. Das Leitthema der diesjährigen DAFTA wird sein: „Neues BDSG: Konsequenzen aus Datenschutzskandalen und Missmanagement“

Zumindest zwei von drei Novellen des Bundesdatenschutzgesetzes sind unter erheblichem Zeitdruck vor Ende der Legislaturperiode verabschiedet worden. Sie haben den Regelungsbereich des BDSG erheblich erweitert. Zugleich führen die

teilweise komplexen Neuregelungen zu Interpretations- und Umsetzungsproblemen. Insbesondere die sogenannte BDSG-Novelle II, die den Datenschutzskandalen wegen illegalem Adresshandel und unzulässiger Mitarbeiterüberwachung geschuldet war, zieht eine Vielzahl von Rechts- und Praxisfragen nach sich.

Die 33. Datenschutzfachtagung greift die Novellierungen des Bundesdatenschutzgesetzes auf und stellt sie auf den Prüfstand der praktischen Umsetzbarkeit. Sämtliche Themenschwerpunkte der drei Novellen werden in Workshops aufgearbeitet und Lösungsmöglichkeiten, die

sich in den Monaten nach Inkrafttreten der Novellierungen anbieten bzw. schon bewährt haben, aufgezeigt. Auch das 28. RDV-Forum unter dem Leitthema „Brennpunkt Mitarbeiterüberwachung“ lässt vor dem Hintergrund des neuen § 32 BDSG wieder hochinteressante Fachvorträge und Diskussionen erwarten.

Das Programm der diesjährigen DAFTA können Sie [hier](#) abrufen.

[Hier können Sie sich zur 33. DAFTA anmelden](#)

[Hier melden Sie sich zum 28. RDV-Forum anmelden](#)

Fristlose Kündigung eines Systemadministrators wegen unerlaubtem Zugriff auf E-Mails

Wenn es um die Durchsetzung von Datenschutz und die Einhaltung von Compliance geht, gibt es einen Akteur, der oft genau zwischen den Stühlen steht. Diese Person steht meist im Spannungsverhältnis von Mitarbeiterüberwachung und dem Schutz der personenbezogenen Daten des Arbeitnehmers. Er ist in Linux-Umgebungen mit sog. root-Rechten bzw. in Windows-Netzwerken mit Administratorprivilegien ausgestattet und kann damit im Grunde rein theoretisch auf fast alle personenbezogenen Daten Einsicht nehmen, die in einem Unternehmensnetzwerk zu finden sind: Der IT-Administrator.

Hierbei scheint jedoch ein Administrator ohne Not seine Kompetenzen überschritten zu haben, in dem er in seiner Eigenschaft als Systemverwalter nachweislich Zugriff auf die E-Mails eines Geschäftsführers genommen hat. Diese habe er dann als Ausdruck einem weiteren Geschäftsführer vorgelegt, um damit den Nachweis darüber zu erbringen, dass der Empfänger der E-Mail vertragswidrig gegen seine Dienstpflichten verstoßen habe und damit eine Schädigung des Unternehmens verursacht habe. Der Systemadministrator habe damit unbefugt auf Daten aus dem Personalbereich zugegriffen entschied das LAG München und bestätigte damit die Entscheidung der Vorinstanz (Arbeitsgericht München.)

Dieses für die Praxis wichtige Urteil (vom 8.7.2009 - 11 Sa 54/09) und alle die gesamten Entscheidungsgründe des Gerichtes können Sie in voller Länge hier nachlesen:

Quelle: http://www.arbg.bayern.de/imperial/md/content/1stmas/lag/muenchen/entscheidungen_2009/kammer11/11sa54_09.pdf

Der BGH zum Haftungsrisiko des Compliance Officers

Eine für die Praxis nicht minder relevante und wichtige Entscheidung hat der BGH gefällt. In seinem Urteil vom 17.07.2009 (Az 5 StR 394/08) wurde der Leiter einer Rechtsabteilung und Revision wegen Beihilfe zum Betrug durch Unterlassen zu einer Geldstrafe von 120 Tagessätzen verurteilt.

Das Urteil lässt wichtige Rückschlüsse darüber zu, wann ein persönliches Haftungsrisiko für Compliance Officer angenommen werden kann. Steht eine Strafbarkeit durch Unterlassen zur Entscheidung muss geprüft werden, ob eine Pflicht zum Handeln, die sog. Garantienpflicht, bejaht werden kann. Durch Zurhilfenahme des Gedankens, dass denjenigen, dem Obhutspflichten für eine bestimmte Gefahrenquelle übertragen seien, auch eine Sonderverantwortlichkeit

für die Integrität des von ihm übernommenen Verantwortungsbereichs trifft, bejaht der BGH das Vorliegen einer Garantienstellung aufgrund der Position des Angeklagten als Leiter der Rechtsabteilung und Innenrevision einer Anstalt des öffentlichen Rechts. Im Rahmen des Urteils findet auch eine ausdrückliche Betrachtung des Compliance Officers im nicht-öffentlichen Bereich statt:

„ ... Deren Aufgabengebiet ist die Verhinderung von Rechtsverstößen, insbesondere auch von Straftaten, die aus dem Unternehmen heraus begangen werden und diesem erhebliche Nachteile durch Haftungsrisiken oder Ansehensverlust bringen können (vgl. Bürkle in Hauschka aaO S. 128 ff.). Derartige Beauftragte wird regelmäßig strafrechtlich eine Garantienpflicht im Sinne des § 13 StGB treffen, solche im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern. Dies

ist die notwendige Kehrseite ihrer gegenüber der Unternehmensleitung übernommenen Pflicht, Rechtsverstöße und insbesondere Straftaten zu verhindern (vgl. Kraft/Winkler CCZ 2009, 29, 32). ...“

Die Ausführungen des BGH lassen erkennen, dass die Aufgaben, die einem Compliance Officer zugeschrieben werden, eher weit zu verstehen sind.

Fazit: Konsequenz der Entscheidung für Compliance Officer ist, darauf zu achten, dass ihre Zuständigkeit, Aufgaben und Befugnisse klar geregelt werden. Dies kann etwa im Arbeitsvertrag oder einer Stellenbeschreibung erfolgen. Zudem zeigt das Urteil das mögliche persönliche Haftungsrisiko eines Compliance Officers auf, der gut beraten ist, gegenüber seinem Arbeitgeber auf haftungsbeschränkende Maßnahmen für seine Person zu drängen.

Quelle: *dejure.org*

Staatsanwaltschaft ermittelt gegen Kik

Der Textildiscounter Kik wirbt mit niedrigen Preisen. Dagegen haben weder die Verbraucher was einzuwenden, noch die Arbeitnehmer. Jetzt stellt sich aber heraus, dass auch Datenschutzbewusstsein, zumindest dasjenige, welches man für die Arbeitnehmer hegt, niedrig ist. Und damit kann in diesen Zeiten kein Unternehmen für sich werben. Der Spiegel informiert auf seinem Onlineauftritt, dass der Textildiscounter in den letzten 18 Monaten flächendeckende Nachforschungen bei der Auskunft Creditreform über die Bonität seiner Angestellten angefordert habe. Bezweifelt wird, dass dies in allen 49.000 erfolgten Fällen auch verhältnismäßig war. Auch Bewerber, die nach dem neuen § 3 Absatz 11 BDSG klar unter die Legaldefinition des „Beschäftigten“ fallen, wurde durchleuchtet.

Auf die Anzeige der Datenschutzbeauftragten von Nordrhein-Westfalen hin, die das notwendige berechnete Interesse zur Durchführung der Nachforschungen bezweifelt, wurde die Staatsanwaltschaft aktiv und ermittelt seitdem gegen Kik.

Quelle: *Online-Auftritt Die Welt*

Google und Facebook müssen nachbessern

Vor dem Landgericht Hamburg hat die Verbraucherzentrale Bundesverband (Vzbv) einen Sieg gegen Google und Facebook errungen. Insgesamt sind zehn Klauseln aus den Nutzungsbestimmungen der US-Konzerne für unzulässig erklärt worden. Weitreichende Nutzungsrechte räumten Google sogar die Möglichkeit urheberrechtlich geschützte Werke oder private Dokumente im Internet zu veröffentlichen. Bei Facebook wird die unklare Datenweitergabe kritisiert. Besonders kritisch fanden die Datenschützer, dass nicht nur die Daten des Anwenders selbst, sondern auch die seiner Freunde offengelegt werden.

Zum gesamten Kommentar: [Focus Online](#)

Staatliche Überwachung

Ob für Zwecke der Sensibilisierung für den Datenschutz, der unterhaltsamen Verdeutlichung der möglichen Konsequenzen für Datenschutzfaule, die gebetsmühlenartig „Ich habe nichts zu ver-

bergen“ sagen, wenn man sie auf den nachlässigen Umgang mit ihren eigenen personenbezogenen Daten anspricht oder aber zur bloßen Unterhaltung für Datenschutzinteressierte; dieser über-

aus einprägsam geschriebene Artikel aus dem Onlineauftritt der Zeit könnte Ihnen gefallen...

Quelle: Zeit-Online

Rechtsfolgen von Datenschutz-Pannen

Der neue § 42a BDSG , erinnert an den Security Breach Notification Act (Gesetz zur Offenlegung von Sicherheitsverletzungen) aus den USA und betrifft die Informationspflicht öffentlicher und nicht-öffentlicher Stellen an die zuständige Aufsichtsbehörde sowie den Betroffenen im Falle einer Datenschutzpanne, in deren Rahmen die unrechtmäßige Kenntniserlangung von Daten im Raume steht.

Trend Micro hat gemeinsam mit der Anwaltskanzlei Bird & Bird LLP ein zum kostenlosen Download zur Verfügung stehendes White Paper vorgestellt, das vor allem auf den neuen Paragraph 42a des Bundesdatenschutzgesetzes eingeht. Das Dokument, das Unternehmen jeder Größe und deren Rechtsabteilungen adressiert, erläutert die wichtigsten Rechtsfolgen von Sicherheitspannen, bei denen personenbezogene Daten oder vertrauliche Unternehmensdaten für Außenstehende zugänglich wurden oder sogar an die Öffentlichkeit gelangten.

Quelle: Internetseite Trendmicro

Direktlink zum kompletten Whitepaper als PDF

Telekom erstattet Strafanzeige gegen Vertriebspartner

Die Telekom hat die Datenschutzskandale der letzten Zeit im Unternehmen anscheinend so weit verarbeitet, dass nunmehr diejenigen Vertriebspartner juristisch belangt werden sollen, die gegen Vertragsvereinbarungen verstoßen haben, sich unseriös verhalten haben oder sogar Straftatbestände verwirklicht haben. Interne Untersuchungen hätten ergeben, dass Unterfirmen von Vertriebspartnern ohne Erlaubnis des Konzerns telefonisch neue Kunden geworben haben.

In anderen Fällen kam es nach Angaben der Telekom auch zu unberechtigtem Zugriff auf Kundendaten der Telekom. Als Verantwortliche für den unzulässigen Datenzugriff hat die Telekom mehrere Adresshändler ausgemacht.

Als Konsequenz aus diesen und anderen Datenmissbräuchen durch Vertriebspartner erwachsen diesen nun Strafanzeigen, die Kündigung der Verträge, vertragliche Abmahnungen und in vielen Fällen auch Forderungen auf Rückzahlung von bereits gewährten Provisionen in Höhe von insgesamt 1,5 Millionen Euro.

Quelle : Handelsblatt vom 06.10.09. S. 14
Online (verkürzt) abrufbar unter:

<http://www.handelsblatt.com/unternehmen/lit-medien/telekom-setzt-vertriebspartner-unter-druck;2464829>

Stimmen zum Datenschutz bei der DB Sicherheit

Bei der DB Sicherheit handelt es sich um ein Tochterunternehmen der Deutschen Bahn. RBB Online lässt in dem folgenden Artikel im Rahmen der Sendung „Klartext“ Herrn Michael Stagen, Betriebsrat DB Sicherheit und Klaus-Dieter Hommel, Bundesvorsitzender Verkehrsgewerkschaft GDBA sowie Prof. Peter Gola, Gesellschaft für Datenschutz und Datensicherung, Vorstandsvorsitzender der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) zu den datenschutzrechtlich bedenklichen Vorkommnissen bei dem Tochterunternehmen der Deutschen Bahn zu Wort kommen. Der Vorwurf der im Raume steht:

Die DB Sicherheit wird beschuldigt illegal Krankendaten von Mitarbeitern gesammelt zu haben. Den Artikel sowie das Video dazu können Sie auf der Seite von RBB Online abrufen.

Quelle: RBB Online

Banken kontrollieren Daten beim Geldtausch

Wundern Sie sich nicht, wenn sie beim Wechseln von Geld in einer Sparkasse demnächst nach Ihrem Ausweis gefragt werden. Dies ist nichts ungewöhnliches, zumindest, wenn Sie kein Kunde der Bank sind. Aufgrund einer Änderung des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)

von 2008 sind Geldinstitute verpflichtet den Namen des Wechselnden mit einer Liste von Terrorverdächtigen des Bundeskriminalamtes abzugleichen. Vorgesehen ist die erhöhte Kontrolle zwar bei Geldbeträgen über 15.000 EUR, die Institute haben aber die Möglichkeit bei „verdächtigen“ Kunden auch nach eigenem

Ermessen auch bei Beträgen unter diesem Betrag die Daten abzugleichen. Die Änderungen sind nach einer Übergangsfrist im Mai diesen Jahres in Kraft getreten.

Quelle: Heise Online

Verbraucherzentrale SH und ULD geben Infos zum illegalen Datenhandel

Praktische Tipps und Empfehlungen zu der Frage, wie sich Bürger und Betroffene vor Datenklau schützen und vor allem wie sie sich dagegen wehren können, wenn sich die personenbezogenen Daten bereits verselbständigt haben, finden sich in der 17-seitigen Broschüre des ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) und der Verbraucherzentrale Schleswig-Holstein. Behandelt werden konkrete Fragen wie:

- Wie beschaffen sich Kriminelle Daten?
- Wie werden die Daten zur Abzocke genutzt?
- Wie bekomme ich mein abgebuchtes Geld zurück?
- Welches sind meine Rechte?
- Wer kann mir helfen?

Die nützliche Broschüre mit dem Titel „Illegaler Datenhandel – Das Geschäft mit Ihren Bankdaten“ lässt sich [hier](#) runterladen

<https://www.datenschutzzentrum.de/presse/20090928-illegaler-datenhandel.htm>

Quelle: Pressemitteilung ULD

Neuregelungen der Auftragsdatenverarbeitung nach §11 BDSG

Die GDD hat eine Mustervereinbarung sowie erste praxisorientierte Erläuterungen zur Neuregelung der Auftragsdatenverarbeitung gemäß § 11 BDSG erarbeitet. Die am 01.09.2009 - ohne Übergangsregelung - in Kraft getretene Vorschrift stellt eine Reaktion auf in der Praxis festgestellte Datenschutzmängel bei der Auftragserteilung und -kontrolle dar. Sie stellt neue Anforderungen an die Beauftragung von Datenverarbeitungsdienstleistern und an das damit zusammenhängende Datenschutzmanagement insgesamt. Enumerativ werden nunmehr im Gesetz die schriftlich festzulegenden Bedingungen der Auftragsdatenverarbeitung aufgeführt. Der Auftraggeber hat sich ferner erstmals vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu überzeugen, was aus Gründen der Nachweisbarkeit zu dokumentieren ist. Mängel bei der Auftragserteilung und der Verzicht auf die gebotene Erstkontrolle können mit einem Bußgeld bis zu 50.000 EUR geahndet werden.

Eine erste Analyse der Neuregelungen durch den mit Datenschutzpraktikern und Juristen besetzten GDD-Arbeitskreis „Datenschutz-Praxis“ hat ergeben, dass die Vorschriften zur Auftragsdatenverarbeitung noch zahlreiche Einzelfragen offen lassen. Mit dem nunmehr von dem Arbeitskreis entwickelten Muster „Auftrag gemäß § 11 BDSG“ bietet die GDD eine erste Orientierungshilfe für die Gestaltung der notwendigen Datenschutzvereinbarungen. Angesichts des hohen Bedarfs in der Praxis stellt die GDD das Muster allen Interessierten auf ihrer Website als Word-Datei zur Verfügung.“ Abrufen können Sie das Muster [auf der Seite der Gesellschaft für Datenschutz und Datensicherung \(GDD e.V.\)](#).

Die vollständige digitale Version ist bei DATAKONTEXT erschienen. Weitere Infos erhalten Sie [hier](#)



„Projekt Datenschutz“ ist online

Es ist zwar besorgniserregend, aber bei der Fülle von Datenschutzpannen, die dem interessierten Leser beim Aufschlagen seiner Tageszeitung, beim Zappen durch die Fernsehkanäle, bei der Radio- sendung auf dem Weg zur Arbeit oder aber auch beim gezielten Recherchieren im Internet begegnen, kann man schon mal den Überblick verlieren.

Wer hatte seine Kundendaten nicht im Griff, wer hatte seine Arbeitnehmer aus- spioniert, wie viele Datensätze waren ver- schwunden..? Ist es ein Déjà-vu oder hat sich das gleiche tatsächlich wieder ereig- net? Den Überblick zu wahren ist nicht leicht. Das „Projekt Datenschutz“ sorgt hier für die nötige Übersicht. Es wurde im September 2009 von PR-COM, Agen- tur für strategische Unternehmenskom-

munikation und PR in München, ins Le- ben gerufen und sammelt Datenpannen, Datenskandale und sonstige Datenvor- fälle in Unternehmen, Behörden und Or- ganisationen. Aber auch die Aktivitäten des deutschen und EU-Gesetzgebers hin- sichtlich Datenschutz werden in diesem Projekt dokumentiert, sporadisch auch weitere interessante Datenvorfälle in an- deren Ländern.

PR-COM will mit diesem Projekt alle Be- teiligten sensibilisieren, mit Daten sorg- fältig und verantwortungsvoll umzuge- hen:

1. Unternehmen sollen ihre eigenen und die in ihrem Verantwortungsbereich befindlichen Daten besser schützen. Die Technologien dazu gibt es längst und sie sind ausgereift

2. Bürger sollen ihre privaten Daten nicht bedenkenlos weitergeben, vor allem nicht im Internet oder in sozialen Netzwerken
3. Den Gesetzgebern soll ihr verfassungs- mäßiger Auftrag in Erinnerung gerufen werden. Es geht um nichts weniger als um ein Monitoring zum Grundrecht auf informationelle Selbstbestimmung.

Die Datenbank wird regelmäßig erwei- tert. Dadurch soll eine möglichst vollstän- dige Übersicht von Datenvorfällen der letzten Jahre entstehen. Besucher der Website können ihnen bekannte, nicht aufgeführte Vorfälle melden. Im Mittel- punkt stehen Fälle aus Deutschland. Bei gravierenden Pannen können aber auch Berichte aus anderen EU-Ländern berück- sichtigt werden.

Quelle: Projekt Datenschutz

Fernmeldegeheimnis bedroht?

Das Fernmeldegeheimnis als Ausfluss des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sieht die Süddeutsche Zeitung in ei- nem Artikel vom 24.09.2009 durch die zunehmende Zahl der Telefonü- berwachungen bedroht.

Diese Befürchtung belegt sie mit eindrucksvollen Zahlen. So habe der Staat im Jahr 2008 im Rahmen von 5008 Ermittlungsverfahren Telefone abgehört und Computer angezapft. Dies sei eine Steigerung bundesweit um 11 , in Bayern um dreißig Prozent. Das ganze Ausmaß der inflationär be- triebenen Überwachungen können Sie auch [online nachlesen](#).

Quelle: Sueddeutsche.de

Wie man sich vor Datenmissbrauch schützen kann

Für den Datenschutzbeauftragten keine Neuigkeiten, aber für den datenschutzinteressierten Bürger wichtige Tipps hat die Online-Ausgabe des Spiegels in 10 Punkten kurz zusam- mengefasst. Ziele sind, wie im BDSG selbst schon angesprochen, den Missbrauch durch Da- tenvermeidung und Datensparsamkeit zu minimieren oder zu verhindern.

Quelle: Spiegel-Online

Datenschutzskandal bei der Österreichischen Bundesbahn (Sammeln von Krankenstandsdaten)

Wenn es Probleme hierzulande gibt, schauen viele gerne zu unseren europäischen Nach- barn. Dass die österreichische Bundesbahn ein offensichtlich nicht minder problematisches Verhältnis zum Beschäftigtendatenschutz hat, wird in diesem [Bericht vom ORF](#) deutlich. Ein neidisches Schielen, wie es z.B. bei der Pisa-Studie üblich ist, ist in diesem Fall nicht nötig.

Quelle: Internetauftritt ORF