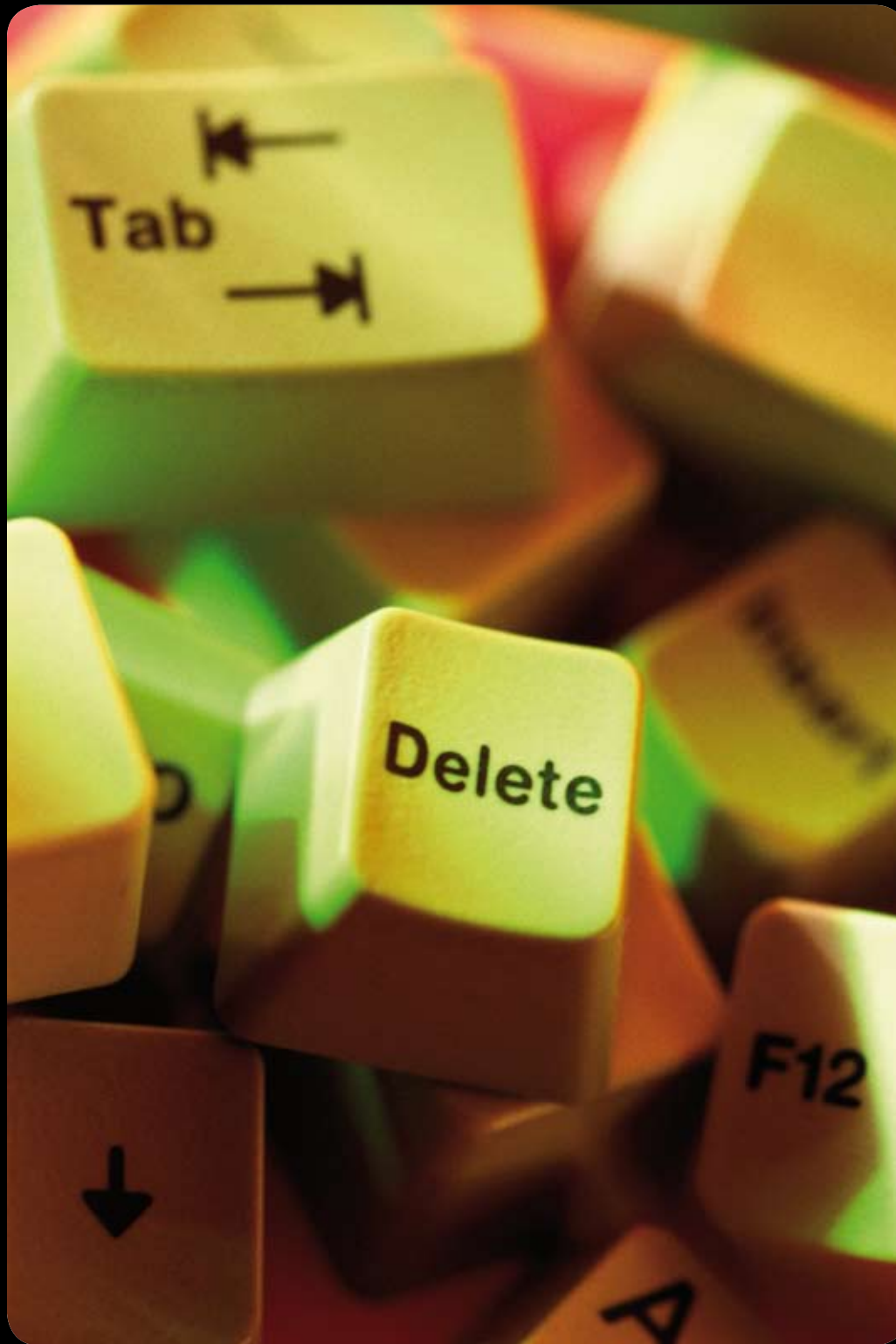


# Datenschutz newsbox



Ausgabe

# 9

09/2010

ULD untersagt Datenübermittlung an Hausärzteverband Schleswig-Holstein .....	3
DoS-Attacke aus der Cloud .....	3
Erstes Modellprojekt zu anonymisierten Bewerbungsverfahren in Deutschland .....	4
Datenlecks, gefährdete Kundendaten und der § 42a BDSG .....	4
Hacker sollen E-Post auf die Probe stellen .....	5
Preisgabe von Staatsgeheimnissen auf XING? .....	5
Bundesinnenminister rät von der Nutzung von Blackberrys ab .....	5
BSI warnt Schwachstelle im mobilen Apple Betriebssystem iOS .....	6
Beschäftigtendatenschutzgesetz verabschiedet .....	6
Bundesnetzagentur verhängt erneut Bußgelder .....	7
Deutsche Post übernimmt Targeting-Spezialisten .....	7
Merkblatt Datenschutz in englischer Sprache lieferbar.....	8
Coaching-Workshop - Datenschutzpraxis .....	8



## Editorial:

„Schwamm drüber!“ So könnte man wohl den Lösungsvorschlag des Google-Chefs Eric Schmidt auf zwei Worte verkürzen, welchen er gegenüber dem Wall Street Journal zum Thema des Problems der zunehmenden Registrierung persönlichen Verhaltens im Internet geäußert hat.

*„I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time,“ he says. He predicts, apparently seriously, that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites.*

Der Google CEO möchte also den „Reset-Knopf“ für Jugendsünden. Auf diesen drückt dann der Jugendliche, wenn er 18 Jahre alt geworden ist und bekommt einen neuen Namen, damit die ganzen Jugendsünden im Netz nicht mehr unter dem alten Namen mit der eigenen Person in Verbindung gebracht werden können.

Das ist natürlich einfacher als den Jugendlichen den sorgsamem und verantwortungsvollen Umgang mit personenbezogenen Daten zu vermitteln und was für den CEO sicherlich viel wichtiger ist: Dieser „Lösungsvorschlag“ lenkt von der Tatsache ab, dass sogar ein Unternehmen, dessen Geschäftsfeld überwiegend darin besteht, Informationen zu sammeln und über das Internet zugänglich zu machen, eine gewisse Verantwortung für den sorgsamem Umgang mit persönlichen Informationen nicht leugnen kann.

Dass auch den sog. „Digital Natives“ klar ist, dass Privatsphäre keine altmodische Erfindung einer analogen Welt ist, glaubt Ihr

RA Levent Ferik  
Gesellschaft für Datenschutz und Datensicherheit e.V.

## ULD untersagt Datenübermittlung an Hausärzteverband Schleswig-Holstein

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein als zuständige Aufsichtsbehörde für die Einhaltung des Datenschutzes im nicht öffentlichen Bereich (§§ 39 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG) in Verbindung mit § 38 Abs. 1 Bundesdatenschutzgesetz [BDSG]) hat gemäß § 38 Abs. 5 BDSG angeordnet, dass es dem Hausärzteverband Schleswig-Holstein e. V. (HÄV SH) unter Androhung eines Zwangsgeldes in Höhe von 30.000 Euro untersagt ist, gemäß dem zwischen der AOK Schleswig-Holstein, dem HÄV SH und Dienstleistern abgeschlossenen Vertrag von eingeschriebenen Hausärzten stammende Patientendaten weiterzugeben oder diese selbst zu nutzen. Die sofortige Vollziehung dieser Verfügung wurde angeordnet.

Damit sind die in der HÄV SH zusammengeschlossenen Hausärztinnen und Hausärzte nicht berechtigt, Abrechnungsdaten auf dem im Vertrag vorgesehenen elektronischen Weg zu übermitteln.

Kern der Auseinandersetzung ist der zum 01.09.2009 novellierte § 11 BDSG, der die sogenannte Auftragsdatenverarbeitung regelt.

Nach § 11 BDSG bleibt bei einer Auftragsdatenverarbeitung der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich und hat durch eine Reihe technischer und organisatorischer Maßnahmen sicherzustellen, dass die Vorgaben des Datenschutzrechts gewahrt werden und auch ein entsprechender schriftlicher Auftrag erteilt wird. Diese gesetzlichen Pflichten verletzen der Hausärzteverband und die teilnehmenden Ärzte nach Auffassung des ULD.

Die Hausärzte hätten faktisch keine ausreichende Möglichkeit der Kontrolle über die Weitergabe von Patientendaten durch ihr Praxissystem. Der Vertrag sehe vor, dass sich die Ärztinnen und Ärzte der HÄV SH als Auftragsdatenverarbeiterin bedienen müssen, wenn sie von den für sie günstigen Hausarzt abrechnungen Gebrauch machen wollen. Tatsächlich seien sie aber weder rechtlich noch faktisch in der Lage, die Kontrolle über ihre Patientendaten als Auftraggeber wahrzunehmen.

An dem Rahmenvertrag, der das Verhältnis zwischen dem Hausärzteverband, Dienstleistern und den einzelnen Ärzten festlegt, seien die Ärzte unmittelbar überhaupt nicht beteiligt. Der Vertrag zwingt die Ärzte dennoch dazu, auf ihren Praxissystemen Software gemäß den Vorgaben des Hausärzteverbandes zu installieren. Den Ärzten werde hierbei sogar vertraglich verboten, Kenntnis von wesentlichen Elementen der Software zu nehmen, so dass sie nach Ansicht des ULD keine vollständige Kontrolle mehr über die Daten auf ihrem System haben. Damit verletzen die Ärzte nach Ansicht des Datenschutzbeauftragten nicht nur ihre Datenschutzpflichten, sondern auch ihre ärztliche Schweigepflicht.

Ein Auftragsverhältnis sei rechtlich zudem dadurch ausgeschlossen, dass der Hausärzteverband, der ausschließlich im Interesse und nach Weisung der einzelnen Ärzte die Daten verarbeiten sollte, ein eigenes Interesse an diesen Daten habe.

Den Text der Verfügung in seinen wesentlichen Zügen finden Sie unter folgend genannter Quelle:

*Quelle: Pressemeldung Unabhängiges Landeszentrum für  
Datenschutz Schleswig-Holstein (ULD)*

## DoS-Attacke aus der Cloud

Dass das Thema Cloud-Computing, insbesondere unter dem Gesichtspunkt der Auftragsdatenverarbeitung einige datenschutzrechtlich interessante Probleme aufwirft, wurde schon oft erwähnt. Ein Bericht von heise-online verdeutlicht, dass Cloud-Computing auch sicherheitstechnische Herausforderungen mit sich bringt.

So haben zwei Sicherheitsexperten nachgewiesen, wie man mit der Infrastruktur eines großen Cloud Computing-Anbieters den Server eines Unternehmens von der Außenwelt abschneiden kann. Für eine Gebühr von 6 Dollar konnten sie ein Programm auf den Servern des Cloud Computing-Anbieters installieren und damit eine Denial-of-Service-Attacke auf das System eines Unternehmens starten.

*Quelle: Heise-Online*

## Erstes Modellprojekt zu anonymisierten Bewerbungsverfahren in Deutschland

Fünf Unternehmen sowie das Bundesfamilienministerium werden sich am Pilotprojekt der Antidiskriminierungsstelle des Bundes (ADS) zu anonymisierten Bewerbungsverfahren beteiligen. Bei den Firmen handelt es sich um die Deutsche Post, die Deutsche Telekom, das Kosmetikunternehmen L'Oréal, den Geschenkdienstleister Mydays und den Konsumgüterkonzern Procter & Gamble. Die beteiligten Unternehmen werden ein Jahr lang anonymisierte Bewerbungsverfahren testen, also Bewerbungen ohne Foto, Name oder Angaben über Alter, Geschlecht, Herkunft und Familienstand, wie die Leiterin der Antidiskriminierungsstelle des Bundes, Christine Lüders, berichtete.

Starten soll der zwölfmonatige Testlauf im Herbst dieses Jahres. Das Pilotprojekt wird während der gesamten Dauer wissenschaftlich begleitet und anschließend ausgewertet. Die beteiligten Unternehmen und Institutionen hatten sich vormals zum Runden Tisch in der unabhängigen Antidiskriminierungsstelle des Bundes getroffen. Dabei wurde unter anderem eine Expertise des Instituts zur Zukunft der Arbeit (IZA) vorgestellt, in der internationale

Modellprojekte verglichen und Handlungsempfehlungen abgeleitet werden. Das IZA ist der wissenschaftliche Kooperationspartner der ADS bei diesem Projekt.

Lüders verwies auf eine beim IZA erschienene Studie von 2010, wonach die Angabe eines türkisch klingenden Namens die Chancen auf eine Einladung zum Vorstellungsgespräch für einen Praktikumsplatz verringert – im Durchschnitt um 14 Prozent, bei kleineren Unternehmen sogar um 24 Prozent. Bei der IZA-Untersuchung wurden Bewerbungen für Praktikumsplätze verschickt. „Wir gehen davon aus, dass die Diskriminierungsquote bei Stellenausschreibungen – vor allem im niedrigqualifizierten Bereich – deutlich höher liegt“, sagte Lüders. „Aber es kann nicht sein, dass Bewerberinnen und Bewerber oftmals nur auf Grund ihres Namens oder ihres Alters keine erste Chance erhalten. Entscheidend für die Auswahl der Bewerberinnen und Bewerber sollte nur die Qualifikation sein. Wir brauchen in Deutschland eine neue Bewerbungskultur.“

*Quelle: Pressemeldung der Antidiskriminierungsstelle des Bundes*

## Datenlecks, gefährdete Kundendaten und der § 42a BDSG

Die Versicherung Alte Leipziger und der Drogerie-Discounter Schlecker machten in den letzten Wochen und Tagen mit Datenlecks von sich reden. Auf einem Server der Versicherung Alte Leipziger standen zeitweise rund 3600 Versicherungsanträge in einem Unterverzeichnis ungeschützt zum Download bereit. Daten wie etwa Bankverbindung, Beruf, Fahrzeuge, eventuelle Vorschäden sowie den bisherigen Versicherer des Antragsstellers konnten von Unberechtigten eingesehen werden. Auch Geburtsdatum, Nationalität, Familienstand und Angaben zu den Kindern fanden sich in den Anträgen. Das Unternehmen gab nach Bekanntwerden des Lecks bekannt, dass man die Betroffenen Kunden zeitnah informieren werde. Das Datenleck beim Drogerie-Discounter offenbarte 150.000 komplette Datensätze von Onlinekunden. Neben Anschrift, Mailadresse und Geburtsdatum ließen die unzureichend geschützten Daten Rückschlüsse auf bestellte Waren zu. Auch hier gab die verantwortliche Stelle an, die betroffenen Kunden umfassend über den Vorfall informieren zu wollen.

Dem aufmerksamen Datenschutzbeauftragten kommen bei diesen Vorfällen mehrere Gedanken in den Sinn:

1. Kann so etwas auch in meinem Unternehmen passieren?
2. Kann so etwas auch bei unserem Auftragsdatenverarbeiter vorkommen?
3. Wie können wir ein solches Datenleck verhindern?
4. Ist das ein Fall des § 42a BDSG?
5. Soweit der § 42a BDSG einschlägig ist: Haben wir einen „Notfall-Plan“ dafür?

*Quelle: Welt.de und heise security*

## Hacker sollen E-Post auf die Probe stellen

Security Cup nennt die Deutsche Post den Wettbewerb im Aufspüren von Sicherheitslücken beim E-Postbrief. Spezialisierte Teams oder Einzelpersonen sollen versuchen, Schwachstellen im System zu entdecken und diese dann melden.

Mit dem E-Postbrief, möchte die Deutsche Post den Kunden eine vertrauliche und verlässliche Kommunikation anbieten. Um diesen Anspruch zu unterstreichen, veranstaltet sie den E-Postbrief Security Cup, in dessen Rahmen unbekannte Schwachstellen im E-Postbrief-Portal auf-

gedeckt werden sollen.

Interessierte Teams müssen sich zuvor bei der Deutschen Post per E-Mail unter [securitycup@deutschepost.de](mailto:securitycup@deutschepost.de) bewerben und versichern, gefundene Sicherheitslücken an die Deutsche Post zu melden. Die Post stellt den Teams dann jeweils alle notwendigen Accounts zur Verfügung.

Zur Bewertung der gefundenen Sicherheitslücken hat die Deutsche Post eine Jury benannt. Dazu gehören bislang der Professor Thorsten Holz von der Ruhr-Universität Bochum und Leiter des deutschen Honey-

net-Projekts, der GSM-Hacker und Netfilter-Entwickler Harald Welte und Professor David Evans von der Universität Virginia.

Mit dem E-Postbrief möchte die Post einen E-Mail-Service etablieren, der rechtsverbindliche Kommunikation beispielsweise mit Behörden ermöglicht. Die Stiftung Warentest kritisierte den Service als teuer, umständlich und nicht absolut sicher. Zumindest letzter Punkt soll wohl nun angegangen werden.

Quelle: Golem.de

## Preisgabe von Staatsgeheimnissen auf XING?

Was würde Ihre Personalabteilung wohl machen, wenn fähiges Personal mit Erfahrung in elektronischer Kampfführung oder mit ausgezeichneten Kenntnissen in der Fernmelde-Aufklärung gesucht würde?

Eine Stellenausschreibung auf der Firmenhomepage? Vielleicht.

Viele würden wohl auch auf dem Business-Netzwerk XING suchen, dachten sich wohl auch einige Ex-Mitarbeiter des Bundesnachrichtendienstes (BND) und haben bei der Suche nach neuen Arbeitgebern über das Social Network mit ihren früheren Tätigkeiten geworben.

Wie aus einem Bericht der Bild hervorgeht, drohen ihnen nun der Verlust von Pensionsansprüchen oder sogar strafrechtliche Konsequenzen. So könnte in einigen Fällen die Grenze zur „Preisgabe von Staatsgeheimnissen“ überschritten worden sein, was Freiheitsstrafen zwischen sechs Monaten und zehn Jahren nach sich ziehen kann.

Die Mitarbeiter des Geheimdienstes sind den Angaben zufolge ihr Leben lang zur Geheimhaltung ihrer früheren Tätigkeit und anderer interner Informationen verpflichtet. Sie dürfen lediglich angeben, dass sie einmal für den BND tätig waren, nicht aber, worin ihre Aufgaben bestanden.

Wenn wir schon bei dem Thema sind:

Haben Sie bereits eine „Social Media Richtlinie“, an die sich Ihre Mitarbeiter richten?

Möglicherweise kann Ihnen der Leitfaden des BVDW einige Anregungen bei der Entwicklung einer solchen Richtlinie geben.

Quelle: Bild.de

## Bundesinnenminister rät von der Nutzung von Blackberrys ab

Bereits im November 2009 hatte der Bundesinnenminister seinen Kollegen in anderen Ressorts in einem Schreiben geraten, am Arbeitsplatz sowohl auf iPhones als auch auf Blackberrys zu verzichten.

Der Bundesinnenminister Thomas de Maizière rät Regierungsmitarbeitern und der Bundesverwaltung nun erneut davon ab, im Dienst Blackberrys zu nutzen. Die Regierung müsse sehr darauf bedacht sein, ihr eigenes Netz wirksam zu schützen, sagte er dem Handelsblatt

„Die Blackberry-Infrastruktur ist ein geschlossenes firmeneigenes System. Den Zugangsstandard zu unseren Netzen muss aber die Regierung selbst bestimmen können und nicht eine Privatfirma“, sagte de Maizière. Insbesondere Regierungsnetze würden immer häufiger von Hackern attackiert.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte im Quartalsbericht 4/2009 auf die Sicherheitsrisiken bei Smartphones hingewiesen. Insbesondere warnte die Behörde vor dem Gebrauch von iPhones und Blackberrys. Sie empfiehlt lediglich das SiMKo2 der Telekom-Großkundensparte T-Systems.

Quelle: Handelsblatt.de

## BSI warnt vor Schwachstelle im mobilen Apple Betriebssystem iOS

Über eine Sicherheitslücke, bei der allein durch das Ansurfen einer bestimmten Website ein iPhone, iPad oder iPod geknackt werden kann, hatte das BSI informiert. Konkret führte das BSI aus: „Bereits das Öffnen einer manipulierten Internetseite beim mobilen Surfen oder das Anklicken eines präparierten PDF-Dokuments reicht aus, um das mobile Gerät mit Schadsoftware zu infizieren. Potenziellen Angreifern ist damit der Zugriff auf das komplette System mit Administratorrechten möglich.“

Mittlerweile können die bekannt gewordenen Sicherheitslücken in den mobilen Geräten iPhone, iPod Touch und iPad des Herstellers Apple können mit einem Sicherheitsupdate geschlossen werden. Bislang stehen Patches für die folgenden Geräte zum Download bereit:

- iOS 4.0.2 für iPhone ab der zweiten Generation (3G, 3GS, 4)

- iOS 4.0.2 für iPod Touch ab der zweiten Generation
- iOS 3.2.2 für iPad

Das BSI empfiehlt, die bereitgestellten Updates schnellstmöglich zu installieren, um eine Ausnutzung der beiden kritischen Schwachstellen im iOS-Betriebssystem zu verhindern. Nach Angaben des BSI ist bislang noch kein Sicherheitsupdate für die iOS Version 3.1.x, die auf dem iPhone und dem iPod Touch der ersten Generation zum Einsatz kommt, veröffentlicht worden. Da inzwischen auch der Code für die mögliche Ausnutzung der beiden Schwachstellen im Internet veröffentlicht wurde, sind diese Geräte weiterhin ungeschützt. Weitere Informationen zu Gefahren und Schutzmöglichkeiten finden Sie in der FAQ des BSI.

*Quelle: Pressemeldung des Bundesamts für Sicherheit in der Informationstechnik (BSI)*

## Gesetzesentwurf zum Beschäftigtendatenschutzgesetz verabschiedet

Nach den Datenschutzskandalen der vergangenen Jahre hat die Bundesregierung einen Gesetzesentwurf zum Beschäftigtendatenschutz verabschiedet, mit dem erstmals der Umgang mit Beschäftigtendaten gesetzlich geregelt wird. Das Kabinett beschloss am 25.08.2010 in Berlin einen entsprechenden Gesetzesentwurf.

Das Thema Beschäftigtendatenschutz umfasst unterschiedliche Themen wie den Umgang mit Bewerberdaten, Verkehrs- und Inhaltsdaten bei der Nutzung von Telefon, E-Mail und Internet am Arbeitsplatz, Gesundheitsuntersuchungen, Datenscreenings zur Erfüllung von Compliance-Anforderungen, Videoüberwachung, Ortungssysteme und biometrische Verfahren.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Peter Schaar, erklärt zum Gesetzesentwurf:

„Mit dieser längst überfälligen Regelung ist ein wesentlicher Schritt hin zu mehr Klarheit im Umgang mit Beschäftigtendaten erfolgt. Es handelt sich aus Sicht des Datenschutzes für Beschäftigte wie für Arbeitgeber um einen tragfähigen Kompromiss, der eine substantielle Verbesserung gegenüber dem Status quo im Umgang mit Beschäftigtendaten darstellt.“ Arbeitgeberpräsident Dr. Dieter Hundt hingegen findet den Gesetzesentwurf eher unzureichend und mit wesentlichen Mängeln behaftet.

*Quelle: Pressemitteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)*

*Quelle: Pressemitteilung der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA)*

## Bundesnetzagentur verhängt erneut Bußgelder

**Die Bundesnetzagentur hat einmal mehr Bußgeld wegen unerlaubter Telefonwerbung verhängt. Die Behörde fordert in zwei Fällen zusammen rund 194.000 Euro und stellt klar: Allgemein vorformulierte Teilnahmebedingungen für Gewinnspiele im Internet sind keine ausreichende Einwilligung für Werbeanrufer.**

Die beiden Bußgeldverfahren umfassen mehrere Beschwerden von Verbrauchern und damit mehrere Taten. Beworben

wurden Produkte aus den Branchen Medien und Versandhandel mit Nahrungsmitteln.

In den Bußgeldverfahren hatten sich die betroffenen Unternehmen auf angebliche Einwilligungserklärungen von Verbrauchern in telefonische Werbung berufen. Bei den vorgelegten Erklärungen handelte es sich um allgemein vorformulierte Teilnahmebedingungen für Gewinnspiele im Internet, die auch Einwilligungen in Telefonwerbung z. B. von Partnern, Sponsoren und sonstigen Unternehmen umfassten.

„Diese Teilnahmebedingungen genügten

den rechtlichen Anforderungen nicht. Für die konkreten Taten lagen somit keine wirksamen Einwilligungen der Angerufenen vor“, betonte Matthias Kurth, Präsident der Bundesnetzagentur. „Wer Werbeanrufer durchführt, ohne über die erforderliche ausdrückliche und wirksame Einwilligung der Verbraucher zu verfügen, dem drohen hohe Bußgelder. Dies zeigen die aktuellen Fälle. Auch in Zukunft werden wir zum Schutz der Verbraucher konsequent gegen Unternehmen vorgehen, die das Verbot unerlaubter Telefonwerbung missachten.“

*Quelle: Pressemeldung der Bundesnetzagentur*

## Deutsche Post übernimmt Targeting-Spezialisten

Die nugg.ad AG ist vielen Datenschützern, die sich mit dem Thema Kundendatenschutz bzw. Online-Marketing befassen, ein Begriff.

Die 2006 gegründete Berliner Nugg.ad bietet mit dem sogenannten Behavioral Targeting gezielte Adressierung der Online-Werbung, die sich an den Interessen der Internetnutzer ausrichten soll – eine Technik, die bei Internetnutzern immer wieder auf starke Bedenken wegen des Erstellens von Nutzerprofilen und Protokollierung des Nutzerverhaltens stößt.

Die Einhaltung des Datenschutzes soll ein Siegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein sicherstellen, das die Technik geprüft hat.

Die Deutsche Post AG hat die nugg.ad AG nun übernommen und möchte mit der Übernahme ihre Kompetenz als Dienstleister im Onlinewerbemarkt erweitern.

*Quelle: Pressemitteilung nugg.ad AG*

## Merkblatt Datenschutz in englischer Sprache lieferbar



**Das Merkblatt Datenschutz ist nun auch in englischer Sprache erhältlich und soll die englischsprachige Mitarbeiter für das Thema Datenschutz sensibilisieren und sie mit den zugehörigen Anforderungen im Unternehmen vertraut machen. Besonders hervorzuheben ist die neue, leicht verständliche Auf-**

**bereitung. In Zusammenarbeit mit Anwendern und Illustratoren ist es der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) gelungen, diese komplexe Materie anschaulich und didaktisch durchdacht zu vermitteln.**

Besonders herausgearbeitet wurde die Verantwortung des gesamten Unternehmens für den datenschutzkonformen Umgang mit personenbezogenen Daten. Hier sind neben der Geschäftsführung auch die Führungskräfte und Mitarbeiter für die Rechtmäßigkeit des Umgangs mit Mitarbeiter-, Kunden- und Lieferantendaten verantwortlich.

Die klare Strukturierung mit Blick auf die Rolle des Staates, des Betroffenen und des Unternehmens sowie die detaillierte Beschreibung der Verantwortlichkeit der

Mitarbeiter sensibilisiert die Beschäftigten erneut für ihre wesentlichen Aufgaben und Pflichten mit Datenschutzbezug. Der abschließende Datenschutz-Know-how-Check gibt den Mitarbeitern die Gelegenheit, das notwendige Datenschutzwissen selbst zu überprüfen.

Das Merkblatt ist ideal für alle Mitarbeiter und für Auszubildende. Schneller und günstiger als jede E-Learning-Lösung. Im Lichte der steigenden Bedeutung des Datenschutzes in den Unternehmen und in der Wirtschaft empfiehlt es sich, dieses Thema neu auf die Tagesordnung zu rufen.

Weitere Information und die Möglichkeit, ein kostenloses Merkblatt-Muster abzufordern finden Sie auf der [DATAKONTEXT-Homepage](#).

## Coaching-Workshop - Datenschutzpraxis

Am 04./05. Oktober findet in Köln ein Workshop für neu bestellte Datenschutzbeauftragte statt. In diesem Workshop werden Teilnehmerfragen von betrieblichen und erfahrenen Praktikern beantwortet und Schwerpunktthemen von den Referenten in Kurzvorträgen vertieft. Darüber hinaus werden eine Vielzahl von Checklisten und Mustern vorgestellt und überlassen, welche die Teilnehmer dann unkompliziert an konkrete Situationen anpassen können. Der Workshop eignet sich auch für Praktiker, um Kenntnisse zur Vorbereitung auf die Prüfung zum GDDcert. aufzufrischen.

Themen u. a.:

- Organisation des Arbeitnehmerdatenschutzes § 32 BDSG
- Die Auftragsdatenverarbeitung nach § 11 BDSG
- Die neuen Spielregeln bei Kundenwerbung
- Prüfpraxis der Aufsichtsbehörden
- Datenschutz versus Compliance
- Neue Herausforderungen (Datenschutz in Communitys)

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