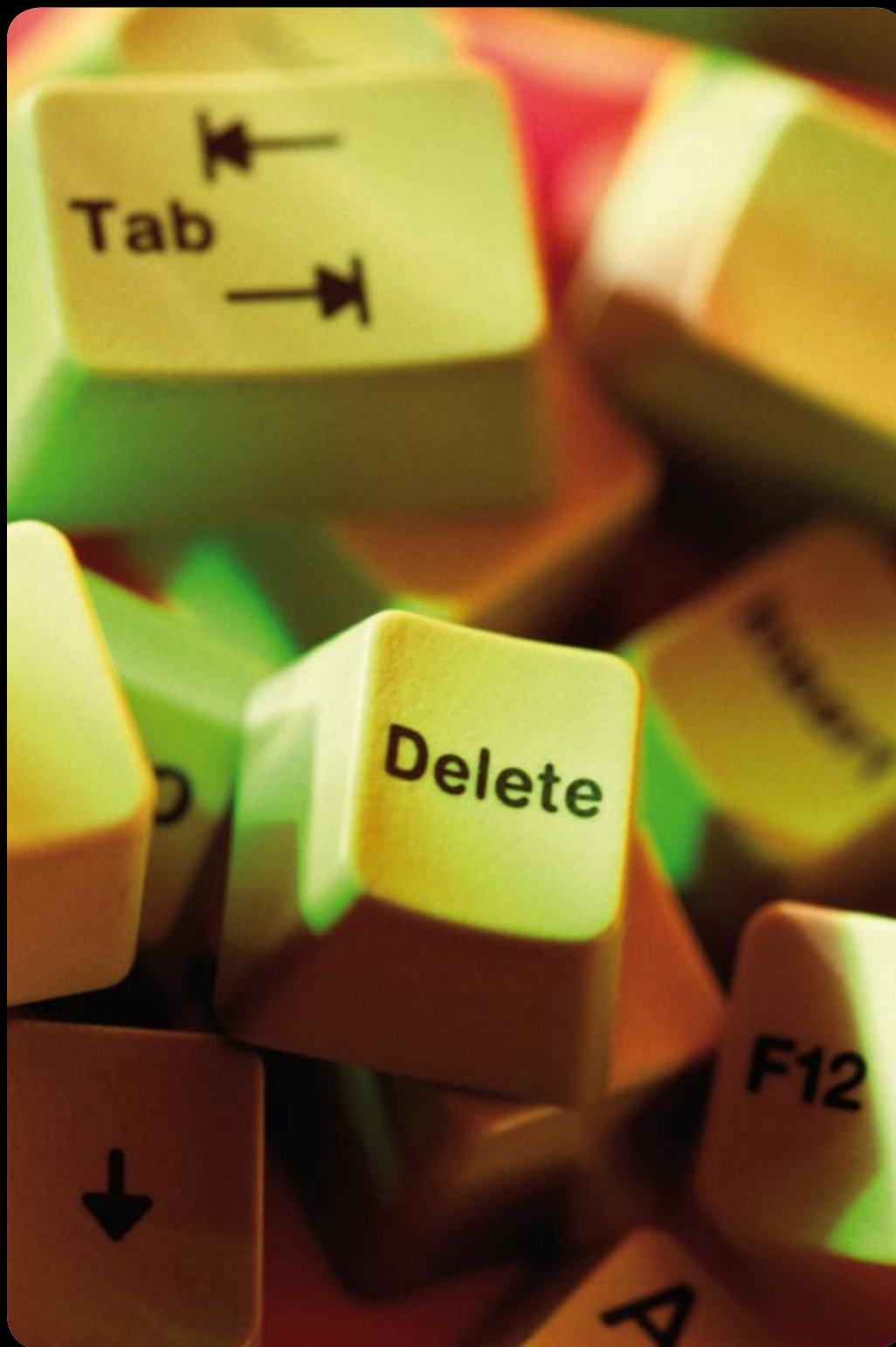


# Datenschutz newsbox



Ausgabe

1

01/2009

Streit zwischen Hamburger Datenschützer und Google dauert an ..... 2  
Aktuelles zum Scoring ..... 3  
Kostenloses eBook "Internetrecht" zum Download ..... 3  
Bevölkerung hat kein Vertrauen in den Datenschutz .... 3

Bundesverfassungsgericht zu Mikado: Kreditkarten-  
screening war erlaubt ..... 4  
Neu entwickelter Algorithmus ermöglicht anonymen  
Datenabgleich ..... 4  
PGP verbessert Diebstahlschutz für Notebooks ..... 4

Pseudonymisierung von Gesundheitsdaten nach neu-  
em ISO-Standard ..... 5  
Bundessozialgericht: Weitergabe von Patientendaten  
an private Abrechnungsstellen unzulässig ..... 5



## Editorial:

Datenschutz in Unternehmen aber auch für den Einzelnen gewinnt weiter mehr an Bedeutung.

Um den Datenschutz erfolgreich umsetzen zu können, ist es unter anderem nötig, auf dem aktuellen Stand der Dinge zu sein, was wesentliche Entwicklungen in diesem Bereich angeht. Mit der steigenden Bedeutung des Datenschutzes wird aber auch die Medienlandschaft rund um den Datenschutz immer unübersichtlicher. An dieser Stelle möchten wir Ihnen Hilfestellung geben.

Der neue Datenschutz-Newsletter von Datakontext informiert Sie in regelmäßigen Abständen umfassend und kompetent über aktuelle Nachrichten, Entscheidungen sowie Entwicklungen im Bereich des Datenschutzes.

Ihr Levent Ferik

Chefredakteur

## Streit zwischen Hamburger Datenschützer und Google dauert an

*Der Streit zwischen Google und dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Johannes Caspar, ist immer noch nicht beigelegt.*

Der Streit dreht sich um die in Google-Maps integrierte Funktion mit dem Namen Google Street View. Das für den Dienst benötigte Kartenmaterial wird von Fahrzeugen herangetragen, die ausgestattet mit mehreren Kameralinsen durch Städte und Ortschaften fahren und dabei Häuser, Straßen und auch Personen erfassen. Diese Bilder von ganzen Straßenzügen sind anschließend im Internet abrufbar. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit bemängelt im Kern die mangelnde Berücksichtigung, Widersprüche Betroffener auch auf die Rohdaten zu erstrecken.

Dazu Prof. Dr. Caspar: „Der wirksame Schutz der personenbezogenen Daten macht es erforderlich, dass die Kamerafahrten ohne Zusage einer kurzfristigen Löschung nicht mehr fortgeführt werden. Gerade vor dem Hintergrund, dass sich die Rohdaten in den USA befinden, kann nicht ausgeschlossen werden, dass sie künftig auch zu anderen als den vorgesehenen Zwecken Verwendung finden. Ich sehe allerdings juristisch keine Möglichkeit, die Fahrten selbst unmittelbar zu verbieten. Denn direkte Eingriffsmöglichkeiten sieht das limitierte Instrumentarium des Bundesdatenschutzgesetzes, das ursprünglich aus den 1970er Jahren stammt, nicht vor. Wir haben als Aufsichtsbehörde nur die Möglichkeit, eine Lösungsanordnung zu erlassen. Diese wird gegenwärtig vorbereitet. Die straßen- und ordnungsrechtlich zuständigen Landesbehörden haben darüber hinaus eigenständig zu prüfen, ob zur Sicherung des informationellen Selbstbestimmungsrechts ihrer Bürgerinnen und Bürger die rechtswidrigen Kamerafahrten künftig untersagt werden müssen.“

Caspar betonte, dass der Verlauf der Verhandlungen mit Google „noch Raum für eine einvernehmliche Lösung“ lasse. Obwohl er offen für weitere Gespräche bleibe, sei er aber entschlossen, „die rechtlichen Optionen auszuschöpfen“.

*Quelle: Internetauftritt des Hamburgischen Beauftragten für  
Datenschutz und Informationsfreiheit 04.06.2009*

## Aktuelles zum Scoring

***In seiner Plenarsitzung vom 12.06.2009 hat auch der Bundesrat einer strengeren gesetzlichen Regulierung von Auskunfteien zugestimmt.***

Eine Zustimmung hatte der Gesetzesentwurf bereits Ende Mai vom Bundestag erhalten. Auskunfteien bzw. Unternehmen, die Informationen über die tatsächliche oder vermeintliche Zahlungsfähigkeit von Privatpersonen sammeln und verkaufen, müssen in allgemein verständlicher Form über die Entstehung der statistischen Werte informieren. Betroffenen wird das Recht eingeräumt Auskünfte über die Gründe der für sie ungünstigen automatischen Einstufung zu erhalten, soweit mathematisch-statistische Verfahren eingesetzt werden. Weitere Möglichkeit den eigenen Scorewert positiv zu beeinflussen, ist die sogenannte „Nachberichtspflicht“. Danach müssen z.B. Kreditinstitute Tatsachen wie eine vorzeitige Schuldentrückzahlung bei Auskunfteien nachmelden. Dadurch erhofft man sich einen positiven Einfluss auf den Scorewert. Zuwiderhandlungen gegen die Nachberichtspflicht können mit einem Bußgeld geahndet werden. Eine Einschränkung hat die Klausel erfahren, wonach Auskunfteien Wohnortdaten in die Ermittlung der Scorewerte zur Prüfung der Kreditwürdigkeit einbeziehen dürfen. Nicht zulässig ist danach die Nutzung von Anschriftendaten für die relevante Wahrscheinlichkeitsberechnung, wenn sich diese ausschließlich auf dieses Datum stützt. Das Gesetz soll am 1. April 2010 in Kraft treten.

Quelle: Virtuelles Datenschutzbüro 12.06.2009 DIP: (Dokumentations- und Informationssystem für Parlamentarische Vorgänge)

## Kostenloses eBook „Internetrecht“ zum Download

***Das bekannte Skript „Internetrecht“ des Münsteraner Jura-Professors Dr. Thomas Hoeren ist in seiner neuesten Version erschienen***

Alle Jahre wieder: Die neue Fassung des bekannten und bewährten Skripts „Internetrecht“ des Münsteraner Jura-Professors Dr. Thomas Hoeren wurde auf den Stand März 2009 gebracht und steht ab sofort auf der Website des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster zum Download als PDF-Datei bereit. Das kostenlos angebotene Kompendium liegt nun in der zwölften Ver-

sion vor. Nach Angaben des Autors haben 200 neue Urteile Eingang in das beliebte Skript gefunden. Dabei wurden Felder, die an Bedeutung verloren haben, wie z.B. „Dialer“ aus dem Skript gestrichen und dafür neu aufgetauchte Phänomene wie das Phishing aufgenommen. Zur Aktualität des Skripts trägt auch die Berücksichtigung der neuen Gesetzeslage bei. Datenschützer werden sich besonders über die Einarbeitung der aktuellen Debatte über neue Richtlinien und Gesetze in Sachen Datenschutz und Internethaftung interessieren.

Quelle:  
ITM Zivilrechtliche Abteilung Prof.  
Dr. Thomas Hoeren

## Bevölkerung hat kein Vertrauen in den Datenschutz

***Eine besorgniserregende Zahl hat eine Umfrage des Instituts für Demoskopie Allensbach zu Tage gebracht.***

Nach einer aktuellen Umfrage glaubt nicht einmal jeder zwölfte Deutsche an den ausreichenden Schutz der bei den Unternehmen gespeicherten Daten. Dass dieses Misstrauen höchstwahrscheinlich ein Ergebnis der zahlreichen Datenschutzaffären der jüngeren Vergangenheit ist, wird nicht von der Hand zu weisen sein.

Aber nicht nur die Unternehmen scheinen in der Gunst der Bürger gefallen zu sein. 72 % der Befragten waren auch hinsichtlich des Staates nicht der Meinung, dass dieser im Umgang mit den gespeicherten Daten als vertrauenswürdig zu betrachten ist. Einzig „positiver“ Effekt der Datenschutzvorfälle der letzten Monate scheint die Sensibilisierung der Bürger im Umgang mit den eigenen personenbezogenen Daten zu sein. So gaben 52 % der insgesamt 1677 Befragten Personen ab 16 Jahren an, dass sie vorsichtiger bei der Angabe ihrer persönlichen Daten geworden seien.

Quelle: IfD Institut für Demoskopie Allensbach  
(Zu wenig Datenschutz?, Nr.6 2009)

## Bundesverfassungsgericht zu Mikado: Kreditkartenscreening war erlaubt

**Das Bundesverfassungsgericht hat die Verfassungsbeschwerde gegen die Aktion "Mikado" nicht zur Entscheidung angenommen.**

Die Daten von 22 Millionen deutschen Kreditkartenbesitzern durften bei Kinderporno-Ermittlungen überprüft werden. Dies hat jetzt das Bundesverfassungsgericht entschieden.

Die Staatsanwaltschaft Halle leitete im Jahr 2006 ein Ermittlungsverfahren gegen Unbekannt ein, nachdem sie auf eine Internetseite aufmerksam geworden war, die den Zugang zu kinderpornografischen Inhalten vermittelte. Der Zugang zur Internetseite kostete 79,99 \$, die von den Kunden per Kreditkarte gezahlt werden mussten. Im Rahmen des Ermittlungsverfahrens schrieb der ermittelnde Staatsanwalt die Kreditinstitute

an, die Mastercard- und Visa-Kreditkarten in Deutschland ausgeben. Er forderte sie auf, alle Kreditkartenkonten anzugeben, die seit dem 1. März 2006 eine Abbuchung von 79,99 \$ zugunsten der philippinischen Bank aufwiesen, über die der Geldtransfer für den Betreiber der Internetseite unter einer bestimmten Empfänger-Kennziffer abgewickelt wurde. Die Unternehmen ermittelten insgesamt 322 Karteninhaber, deren Daten an die Staatsanwaltschaft weitergegeben wurden. Eine Verletzung des von den Beschwerdeführern gerügten Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG sah das Verfassungsgericht nicht.

Nach Auffassung des Bundesverfassungsgerichts liege schon kein Eingriff in dieses Grundrecht vor, da nur die Daten der 322

Verdächtigen an die Polizei weitergegeben wurden. Die Daten der übrigen Millionen Menschen seien bei den Banken nur „anonym und spurenlos“ überprüft worden. Karlsruhe hielt auch kein neues Gesetz für die Kreditkartenfahndung für erforderlich. Die Maßnahme beruhe auf der Ermittlungsgeneralklausel des § 161 Abs. 1 StPO. Die Übermittlung von Daten jener Kreditkarteninhaber, welche die Tatkriterien erfüllten, berühre diese zwar in ihrem Recht auf informationelle Selbstbestimmung, § 161 Abs. 1 StPO sei jedoch eine hinreichend bestimmte Rechtsgrundlage für diesen Eingriff, da die Norm Ermittlungen und damit auch die Datenerhebung auf den Zweck der Tataufklärung begrenze.

*Bundesverfassungsgericht: Az. 2 BvR 1372/07,  
2 BvR 1745/07*

## Neu entwickelter Algorithmus ermöglicht anonymen Datenabgleich

Ob sich der von Andrew Yehuda Lindell, Juniorprofessor für Computerwissenschaften an der israelischen Bar-Ilan University, entwickelte Algorithmus auch für einen datenschutzkonformen Umgang mit Datenbanken, die einem Abgleich zugeführt werden sollen, verwenden ließe, muß sich noch zeigen. Mit diesem sollen sich zwei Datenbanken anonym miteinander abgleichen lassen. Der Algorithmus wurde aus der Idee geboren, dass zwei Organisationen, die sich gegenseitig nicht vertrauen, die Möglichkeit erhalten sollen, zu ermitteln, ob beide über den gleichen Datenbestand verfügen.

Mehr zum Thema in Technology Review online:  
<http://www.heise.de/newsticker/Datenvergleich-ohne-Offenlegung-privater-Informationen--Imeldung/135300>

## PGP verbessert Diebstahlschutz für Notebooks

**Der Krypto-Spezialist PGP hat eine Software entwickelt, die auf der Anti-Theft genannten Technik von Intel aufbaut. Dabei soll der von Intel entwickelte Hardware-Schutz mit der hauseigenen Notebook-Software „Whole Disk Encryption“ verschmelzen.**

Durch die neue Technik wird zwar nicht der Diebstahl eines Notebooks verhindert, jedoch bleiben die meist sensiblen Daten, die den materiellen Wert des Geräts in fast jedem Fall übersteigen werden, vor unberechtigtem Zugriff geschützt. Die gespeicherten Daten werden bei einem Verlust des Geräts mit einer PGP-Verschlüsselung geschützt. Das System kann auch so konfiguriert werden, dass nach mehrmaliger falscher Eingabe des Boot-Passworts oder alternativ nach längerem Kontaktverlust mit einem festgelegten Server der Zugriff auf die Festplatte des Notebooks verhindert wird. Es besteht jedoch die Möglichkeit, dass ein einmal blockiertes Gerät reaktiviert werden kann, wenn es zu seinem rechtmäßigen Eigentümer zurückkehren sollte.

*Quelle: Heise iX Online - PGP integriert Intels Diebstahlschutz für Notebooks*

## Pseudonymisierung von Gesundheitsdaten nach neuem ISO-Standard

**Die International Organization for Standardization hat am 10.03.2009 die neue ISO-Spezifikation (ISO/TS 25237:2008) zur Pseudonymisierung von Gesundheitsdaten veröffentlicht.**

Da im Gesundheitswesen oftmals sehr sensible personenbezogene Daten verarbeitet werden, bietet sich in diesem Bereich

die sog. Pseudonymisierung als datenschutzfreundliche Maßnahme an, um dem steigenden Bedürfnis nach Schutz dieser Daten gerecht zu werden und die gesetzlichen Vorschriften einzuhalten.

Unter Pseudonymisieren versteht man das „Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“ (vgl. § 3 Abs. 6a BDSG).

Soweit diese Daten jedoch für Forschungszwecke genutzt werden sollen, macht der Zweck einen Personenbezug entbehrlich. Diese Spezifikation behandelt daher den Schutz von u.a. Patientendaten, aber auch Daten von in Heilberufen tätigen Personen oder Daten von Krankenhäusern.

Quelle:  
*International Organization for Standardization*

## Bundessozialgericht: Weitergabe von Patientendaten an private Abrechnungsstellen unzulässig

**Das Bundessozialgericht hat über die Zulässigkeit der Weitergabe von Patientendaten im Krankenhaus behandelter Patienten an private Abrechnungsstellen in der gesetzlichen Krankenversicherung entschieden.**

Dem Urteil lag die Klage eines Klinikums zugrunde, welches Abrechnungen für Notfallbehandlungen nicht mehr selbst vornahm, sondern an eine privatärztliche Abrechnungsstelle weitergab.

Das jederzeit widerrufliche Einverständnis mit der Verarbeitung Ihrer Daten bei der Abrechnungsstelle erklärten die Patienten mit der Unterzeichnung einer Ihnen vorgelegten Erklärung. Die Vergütung der so zustande gekommenen Abrechnung wurde nicht von der beklagten kassenärztlichen Vereinigung akzeptiert und daher nicht vergütet.

Sozialgericht und Landessozialgericht gaben dem klagenden Klinikum Recht. Vor dem BSG unterlag es jedoch.

Das hat zur Folge, dass nach gegenwärtiger Rechtslage Krankenhäuser oder Vertragsärzte keine Patientendaten an private Dienstleistungsunternehmen zur Erstellung der Leistungsabrechnung übermitteln dürfen. Dies gilt auch, wenn die Patienten Einwilligungserklärungen unterzeichnet haben. Zur Abfederung der durch die Entscheidung zu erwartenden Auswirkungen ist eine Übergangsregelung vorgesehen. Damit kann dieser Entscheidung (B 6 KA 37/07 R) des Bundessozialgerichts eine weitreichende Wirkung beigemessen werden, was den Schutz von Patientendaten in der gesetzlichen Krankenversicherung angeht. Leistungen, die bis zum 30.6.2009 erbracht werden, müssen auch dann von den Kassenärztlichen Vereinigungen vergütet werden, wenn sie unter Verstoß gegen das Verbot der Datenweitergabe an private Stellen abgerechnet wurden.

Quelle: *Datenschutz-Berater 3/2009 S. 19*