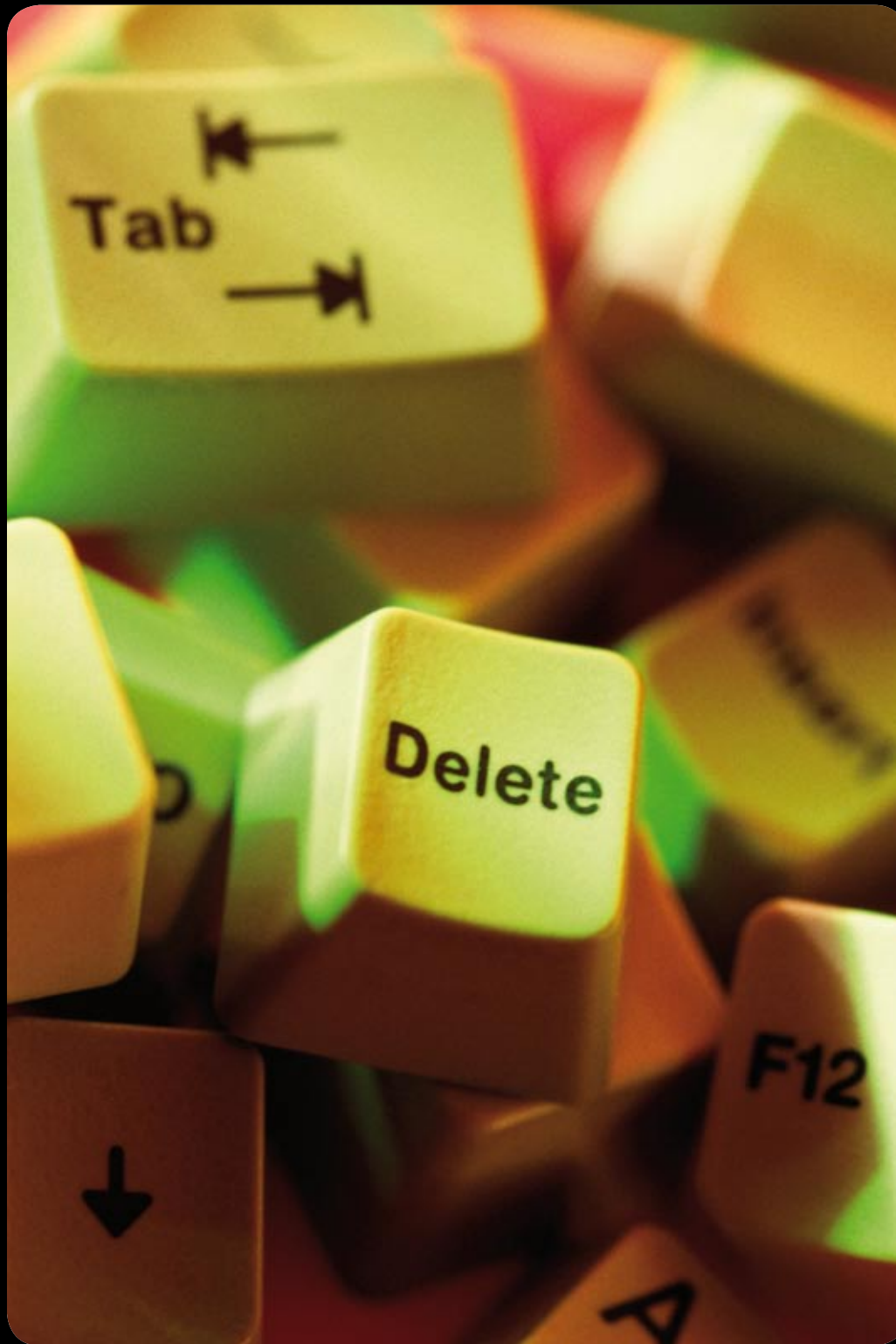


Datenschutz newsbox



Ausgabe

1

01/2010

Mustervertragsanlage zur Auftragsdatenverarbeitung mit englischer Übersetzungshilfe der BITKOM	2
Staatlicher Pflichtschutz vor Schadprogrammen	2
Presseerklärung zu den Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten	3
Unzulässige E-Mail-Werbung gegenüber Geschäftskunden	3
Deutsche Telekom: Datendiebstahl erfordert Austausch von Kundennummern	3
Nessus in Version 4.2 erschienen	4
ULD zertifiziert Systemadministratoren	4
Alle 39.400 Jahre eine Datenschutzprüfung?	5
Beschlüsse des Düsseldorfer Kreises zu Analyseverfahren / Geolokalisierung	5
Dauerüberwachung per Video illegal	5
Baden-Württembergischer Landesbeauftragter für den Datenschutz stellt Tätigkeitsbericht vor	6
Kfz-Scanning grundrechtswidrig?	6
Zulässigkeit verdeckter Bonitätsprüfungen	6
Elena alarmiert Datenschützer	7
Informationsschrift „Datenauswertung und personenbezogene Datenanalyse“	7
ENISA-Studie hilft bei Risikoabschätzung für Cloud Computing	8
Datenschutz Best Practice in fünfter Auflage lieferbar ..	8
Die Datenpanne! Albtraum jedes Unternehmens	8



Editorial:

Ein nicht nur in datenschutzrechtlicher Hinsicht ereignisreiches Jahr liegt hinter uns. Was viele noch zur Mitte des letzten Jahres für nicht mehr möglich hielten, wurde kurz darauf doch noch in die Tat umgesetzt. Das Bundesdatenschutzgesetz wurde um viele Punkte ergänzt und bescherte lange vor Weihnachten allen Interessierten eine reichhaltige Bescherung.

Was das neue Jahr an schönen und weniger schönen Überraschungen bereit hält, ist noch nicht abzusehen. Für die Datenschutzbeauftragten haben die Novellen des Jahres 2009 genug neue Fragen aufgeworfen, die einer Antwort bedürfen. Viele Prozesse müssen neu überdacht und an die sich geänderten Anforderungen angepasst werden. Viel Erfolg und Spaß bei Bewältigung der vor Ihnen liegenden Aufgaben wünscht Ihnen Ihr

Levent Ferik

Mustervertragsanlage zur Auftragsdatenverarbeitung mit englischer Übersetzungshilfe der BITKOM

Die Auslagerung von Datenverarbeitungsprozessen oder deren Übertragung auf eine unternehmensfremde Stelle ist für viele Unternehmen eine wichtige Möglichkeit, externes Know-how nutzen und gleichzeitig Kosten sparen zu können. An die Auftragsdatenverarbeitung stellt das Bundesdatenschutzgesetz hohe Anforderungen, deren Missachtung Sanktionen nach sich ziehen können.

Nach dem das Regierungspräsidium Darmstadt und die Gesellschaft für Datenschutz und Datensicherung (GDD e.V.) einen Mustervertrag zur Auftragsdatenverarbeitung nach dem neuen § 11 BDSG der Öffentlichkeit zur Verfügung gestellt haben, hat nun auch die BITKOM einen solchen Vertrag auf Ihrer Internetseite zum freien Download bereit gestellt. Der Mustervertrag enthält zusätzlich eine englische Übersetzungshilfe. Es sollte jedoch beachtet werden, dass der englische Text in der rechten Spalte nicht zur Verwendung als Vertragsinhalt gedacht ist, sondern lediglich eine Übersetzungshilfe zu der deutschen Mustervertragsanlage darstellt.

Quelle: BITKOM

Staatlicher Pflichtschutz vor Schadprogrammen

Zur Bekämpfung von Botnetzen richtet der eco – Verband der deutschen Internetwirtschaft mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein providerübergreifendes Beratungszentrum ein. Kunden von Internet Service Providern erhalten darüber zukünftig professionelle Unterstützung, wie sie Schadprogramme von ihren Rechnern entfernen können. eco stellte das Projekt beim vierten nationalen IT-Gipfel in Stuttgart vor. Schon in der ersten Jahreshälfte 2010 sollen PC-Nutzer auf die Hilfe der Beratungsstelle zurückgreifen dürfen, mit der sie ihre Rechner daheim von Computerviren befreien können.

Im Rahmen des zentralen Beratungszentrums werden Internet-Zugangsanbieter Kunden, deren Rechner sie als Teil eines Botnetzes identifiziert haben, zunächst auf eine Website leiten, die ihnen Hilfestellungen und Tools zum Entfernen der Malware bereitstellt. In einem zweiten Schritt kann der Provider dem Kunden einen Zugangscode für die telefonische Unterstützung mitteilen. Dort werden Anti-Viren-Spezialisten mit dem Kunden den Schädling aufspüren und entfernen. „Mit dem Projekt möchten wir Deutschland mittelfristig aus den Top 10 der Länder, von denen schädliche Online-Aktivitäten ausgehen, herausbringen“, sagt Sven Karge, Fachbereichsleiter Content bei eco.

Quelle: Pressemeldung BSI und eco

Presseerklärung zu den Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten

Wie steht es um den Datenschutz im Freistaat Sachsen?

Einen guten Rundumblick vermittelt der neu vorgestellte 14. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten Andreas Schurig. Der Bericht ist über 200 Seiten stark, wobei sich die Behörde nach eigenen Angaben mit 425 Sachverhalten zu befassen hatte. Die Bandbreite der dabei behandelten Fälle reicht vom Internetrecht, über Arbeitsrecht bis hin zur Videoüberwachung. In diesem Zusammenhang macht der Sächsische Datenschutzbeauftragte darauf aufmerksam, dass die Videoüberwachung nicht immer hingenommen werden muss. Daher können auch die dargestellten Fälle und die Ausführungen der Behörde für betriebli-

che Datenschutzbeauftragte sinnvolle „Übungsfälle“ sein, um zu vertretbaren Ergebnissen bei der Überprüfung der Zulässigkeit von z.B. Fällen der Videoüberwachung zu gelangen.

Weiteren Nachholbedarf sieht Schurig im Bereich des bewussten Umgangs mit personenbezogenen Daten sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft. Insbesondere im Rahmen der Beantragung von Sozialleistungen wird kritisiert, dass die von den Behörden geforderten personenbezogenen Daten oftmals einem „Daten-Striptease“ gleichkämen.

Quelle: [Internetauftritt des Sächsischen Datenschutzbeauftragten](#)

Unzulässige E-Mail-Werbung gegenüber Geschäftskunden

Marketingaktionen per E-Mail sind in rechtlicher Hinsicht keine triviale Angelegenheit. Das hängt auch damit zusammen, dass im Rahmen einer zulässigen Marketingaktion Anforderungen nicht nur des BDSG, sondern auch des UWG zu beachten sind. Das Landgericht Bonn hat kürzlich eine Entscheidung getroffen, die von Unternehmen, die Ihre Kunden per E-Mail zu Werbezwecken ansprechen, unbedingt berücksichtigt werden sollte.

Ein Kunde des beklagten Unternehmens hatte im Rahmen einer Werbeaktion eine E-Mail bekommen, ohne dass dessen ausdrückliche Einwilligung dazu vorlag. Das Verhalten des Unternehmens wäre ausnahmsweise unschädlich, wenn § 7 Abs. 3 UWG, wonach Werbung per E-Mail auch ohne vorherige Einwilligung erlaubt sein kann, einschlägig gewesen wäre. Dabei müssen aber alle Voraussetzungen des § 7 Abs. 3 UWG kumulativ vorliegen. Dass das Fehlen schon einer Voraussetzung zum Scheitern der Ausnahmeregelung führen kann, zeigt dieses Urteil sehr deutlich. Hierbei hatte das Unternehmen gem. § 7 Abs. 3 Nr. 4 UWG aus einem Versehen heraus vergessen, „den Kunden bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hinzuweisen, dass er der Verwendung jederzeit widersprechen kann, ohne dass dafür andere als die Übermittlungskosten nach den Basistarifen entstehen“. Bei der Auswahl des, im Vergleich zur Briefpost sicherlich kostengünstigeren E-Mail-Versands, sollten werbetreibende Unternehmen eine gewissenhafte rechtliche Prüfung der Zulässigkeit der E-Mail-Werbung nicht vernachlässigen. Den Volltext der Entscheidung finden Sie hier:

Quelle: [MIR \(Medien Internet und Recht\) LG Bonn, Urteil vom 08.09.2009 - Az. 11 O 56/09](#)

Deutsche Telekom: Datendiebstahl erfordert Austausch von Kundennummern

Falls Sie in nächster Zeit von der Deutschen Telekom eine neue Kundennummer erhalten, könnten dies die Nachwehen der massiven Datendiebstähle der Vergangenheit sein. Bei dem geplanten Austausch scheint es sich um eine Maßnahme zur Eindämmung von Missbrauch sein, die in Verbindung mit den gestohlenen Datensätzen auftreten könnten. Durch den Austausch sollen die rund 17 Millionen Kundendaten für die dubiosen Firmen, bei denen die Kundendaten in Umlauf geraten waren wertlos werden.

Quelle: [Spiegel.de](#)

Nessus in Version 4.2 erschienen

Der Schwachstellenscanner Nessus wird denjenigen, die sich auch mit dem technisch-organisatorischen Datenschutz intensiv befassen ein Begriff sein. Bei Nessus handelt es sich um einen Netzwerk- oder Vulnerability Scanner für Linux-, Unix- Windows- und OS X-systeme. Nessus basiert auf dem Client-Server-Prinzip. Das heißt, dass auf einem Rechner der Nessusserver (nessusd) gestartet wird und anschließend die Möglichkeit besteht sich mit einem oder mehreren Clients entweder vom lokalen oder einem entfernten Computer darauf zu verbinden. Abgesichert wird dies durch SSL-Zertifikate und Passwörter.

Mit dem Start des Servers werden automatisch die Plugins geladen. Mit diesen Plugins lassen sich diverse Sicherheitslücken des Betriebssystems bzw. der Dienste, die auf dem zu scannenden Host laufen, finden. Die Plugins werden in der Nessus-eigenen Skriptsprache „Nessus Attack Scripting Language“ (NASL) erstellt.

Mit Hilfe des „Clients“ kann der IT-Admin sich mit dem Server verbinden und eine „Session“ einstellen, in welcher er dann die Plugins, den Zielhost und andere Einstellungen eintragen oder verändern kann. Wurde der Scan auf einen Host ausgeführt, gibt der Nessus-Client eine Übersicht über die offenen Ports (das Scannen der Ports macht Nessus mit nmap) und eventuell gefundene Sicherheitslücken aus.

Damit handelt es sich bei Nessus um ein sehr beliebtes Tool bei Security-Audits.

IT-Admins können das Werkzeug für das Aufspüren von Schwachstellen und das Schließen von Sicherheitslecks in der IT-Struktur nutzen. Dieses nützliche Tool ist nun in einer überarbeiteten Version erschienen.

Übrigens hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Open-Source-Software unter dem Namen BOSS (BSI OSS Security Suite) entwickelt, welche im Wesentlichen auf dem Sicherheits-Scanner Nessus aufbaut.

Die Nutzung für private Zwecke ist kostenlos. Zum Aktivieren ist jedoch die Angabe einer gültigen E-Mail-Adresse erforderlich. Professionelle Nutzer müssen eine Lizenz erwerben, die für 1 Jahr 1200 US-Dollar kostet.

Quelle: [Tenable Network Security](#)

ULD zertifiziert Systemadministratoren

In der Gesamtkonzeption des BDSG, in der Datenschutz durch Technik eine zentrale Rolle spielt, ist der technisch-organisatorische Datenschutz und damit auch der Systemadministrator ein wichtiger Baustein. So ist es ein naheliegender Gedanke, eine Möglichkeit der Zertifizierung für diesen Personenkreis zu bieten.

Das Unabhängige Landeszentrum für Datenschutz (ULD) konnte in diesem Jahr zum sechsten Mal in Folge Systemadministratoren zertifizieren. Mit der bestandenen Prüfung erhielten sie den Titel „Systemadministrator mit Datenschutzzertifikat“.

Geprüfte Systemadministratoren können mit dem Datenschutzzertifikat folgende Kompetenzen nachweisen:

- Fundierte Kenntnisse im Bereich Datenschutzrecht, Systemdatenschutz und Datensicherheit
- Methodische Vorgehensweise beim IT-Sicherheitsmanagement, beim Aufbau und bei der Begutachtung von IT- und Sicherheitskonzepten
- Sichere Verwaltung von Sicherheitsfunktionen der Betriebssysteme Windows Server 2003 und XP
- Entwicklung und Einsatz von datenschutz- und datensicherheitskonformen Strategien bei der Anbindung an externe Netze

Mit dem Erwerb des Datenschutzzertifikats können Systemadministratoren nicht nur ihre persönliche und berufliche Qualifikation verbessern, sie geben auch ihren Arbeitgebern die Sicherheit, dass die vorgeschriebenen technischen, organisatorischen und datenschutzrechtlichen Vorschriften bei der Systemadministration berücksichtigt werden können.

Quelle: [Unabhängiges Landeszentrum für Datenschutz \(ULD\)](#)

Alle 39.400 Jahre eine Datenschutzprüfung?

„Vertrauen ist gut, Kontrolle ist besser!“ ist eine Redewendung, die angeblich von dem russischen Politiker Lenin stammen soll. Wichtig ist in diesem Zusammenhang aber auch nicht die Urheberschaft der Redewendung, sondern ihre Aussage. Diese besagt, man soll sich nur auf das verlassen, was man nachgeprüft hat. Was aber, wenn man rein faktisch gar nicht die Möglichkeit hat angemessen zu prüfen?

Folgt man der Aussage der Redewendung und überträgt das auf die Einhaltung des Datenschutzes und die Überprüfung der Einhaltung durch die Datenschutzaufsichtsbehörden in Deutschland, muss dies

in Konsequenz wohl heißen, dass man sich auf die Einhaltung der datenschutzrechtlichen Vorgaben in den Unternehmen nicht unbedingt verlassen kann. Zu einer ähnlichen Schlussfolgerung kommen auch die Autoren des Xamit Datenschutzbarometers 2009:

Pro 100.000 Unternehmen stehen bundesweit gerade einmal zwei Personen zur Verfügung, die den rechtskonformen Umgang mit personenbezogenen Daten kontrollieren. In Baden-Württemberg beispielsweise bedeutet dies, dass Unternehmen statistisch betrachtet nur etwa alle 39.400 Jahre mit der behördlichen Überprüfung ihrer Datenschutzpraxis rechnen müssen.

Der Datenschutzbarometer zeigt darüberhinaus, wie es um die gesetzlich vorgeschriebene Verpflichtung der Erstellung

eines Verfahrensverzeichnis und der datenschutzgerechten Ausgestaltung der Webpräsenz steht.

Bemerkenswert ist z.B. die Zahl der Webpräsenzen, die durch den Einsatz des Tools Google Analytics ggf. gegen den Datenschutz verstoßen. Immerhin wurde der Einsatz des besagten Tools in einem Gutachten des Datenschutzbeauftragten Schleswig-Holsteins als rechtswidrig eingestuft. Zu der Frage der Zulässigkeit beachten Sie auch den nachfolgenden Beschluss des Düsseldorfer Kreises zu Analyseverfahren.

Die vollständige 47-seitige Studie können Sie auf der Website des Unternehmens kostenlos herunterladen.

Quelle: [XAMIT Bewertungsgesellschaft mbH](#)

Beschlüsse des Düsseldorfer Kreises zu Analyseverfahren / Geolokalisierung

Der Düsseldorfer Kreis (die informelle Vereinigung der obersten Aufsichtsbehörden für den nicht-öffentlichen Bereich (Unternehmen) im Datenschutzrecht) hat seinen neuen Beschluss zur datenschutzkonformen Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten vorgelegt. Insbesondere sollte der letzte Punkt zur Analyse des Nutzungsverhaltens anhand von IP-Adressen (einschließlich Geolokalisierung), die ggf. die Kürzung der IP-Adresse schon vor der Auswertung erfordert, Beachtung finden, da dies bei einigen Produkten zu einer Neubewertung führen kann.

Eine FAQ zu dieser Problematik finden Sie auf den [Seiten des ULD](#).

Lesen Sie auch die rechtliche Bewertung des [Instituts für IT-Recht \(IITR\)](#), das verkürzt zu folgendem Ergebnis in dieser Sache kommt: „Die obersten Datenschutz-Aufsichtsbehörden haben Ende November einen Beschluss erlassen, wonach die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen aufgrund der Personenbeziehbarkeit dieser Daten nur mit bewusster, eindeutiger Einwilligung zulässig sei. Damit ist in der Praxis von der Verwendung von Google Analytics (und ähnlicher Tools) in seiner derzeitigen Form in den meisten Fällen abzuraten.“

Quelle: <http://www.lfd.m-v.de/dschutz/beschlue/Analyse.pdf>

Dauerüberwachung per Video illegal

Nach einer Entscheidung des Oberlandesgerichts Oldenburg ist die Dauerüberwachung von Autobahnen per Video zur Verfolgung von Verkehrsdelikten grundrechtswidrig. Eine solche Überwachung greife schwerwiegend in das allgemeine Persönlichkeitsrecht nach Artikel 1 und 2 der Verfassung dar, stellte das OLG in einem Beschluss fest.

Das Gericht hob mit seiner Entscheidung ein Bußgeld des Kreises Osnabrück auf. Die Behörde wollte einem Autofahrer mit Dauervideoaufnahmen einen zu geringen Abstand zu einem vorausfahrenden Auto nachweisen. Das Beweismittel sei illegal erlangt worden und damit nicht verwertbar, stellten die Richter fest. Die Videoüberwachung verstoße auch gegen die Grundrechte von Autofahrern, die sich auf den Straßen korrekt verhalten, argumentierte der Senat für Bußgeldsachen (AZ.: Ss Bs 186/09).

Quelle: [N-TV.de](#)

Baden-Württembergischer Landesbeauftragter für den Datenschutz stellt Tätigkeitsbericht vor

Auch der Landesbeauftragte für den Datenschutz Baden-Württemberg hat vor kurzem (14.12.2009) seinen Tätigkeitsbericht vorgestellt. In einer ausführlichen Pressemitteilung zum Tätigkeitsbericht macht der Baden-Württembergische Datenschutzbeauftragte u.a. auf Folgendes aufmerksam:

Aufgrund echter oder vermeintlicher Datenschutzskandale sei das Thema Datenschutz in den Medien und in der Öffent-

lichkeit in den zurückliegenden Monaten so präsent gewesen wie selten zuvor. Dies habe zwar in erster Linie den nicht-öffentlichen Bereich betroffen, dennoch habe auch das Vertrauen in den Staat gelitten. „Der demokratische Rechtsstaat ist auf das Vertrauen seiner Bürgerinnen und Bürger angewiesen. Wenn aber 72% der Bevölkerung erklären, sie würden dem Staat hinsichtlich des Umgangs mit ihren Daten misstrauen, dann ist das ein

Alarmsignal“, erklärte der Landesdatenschutzbeauftragte unter Verweis auf eine Umfrage des Instituts für Demoskopie Allensbach...”

Eine ausführliche Pressemitteilung zum Tätigkeitsbericht findet sich unter dem nachfolgenden Link.

Quelle: [Landesbeauftragter für den Datenschutz Baden-Württemberg](#)

Kfz-Scanning grundrechtswidrig?

Ob die automatische Erfassung von Pkw-Kennzeichen in Baden-Württemberg rechtmäßig ist, wird vom Bundesverfassungsgericht im Rahmen einer Verfassungsbeschwerde geprüft. Die Beschwerdeführer kritisieren, das Gesetz lasse „in Abwesenheit jeder Gefahr“ eine automatisierte Massenkontrolle des öffentlichen Straßenverkehrs zu. Autofahrer müssten aufgrund des Kennzeichenabgleichs mit der Erstellung von Bewegungsprofilen rechnen. Die Befugnis sei so unbestimmt und weit gefasst, dass nicht vorhersehbar sei, wann und wie die Polizei von ihr Gebrauch macht. Die vollständige Beschwerdeschrift finden Sie [hier](#).

Quelle: [Daten-Speicherung.de](#)

Zulässigkeit verdeckter Bonitätsprüfungen

Für Datenschutzbeauftragte, die sich mit datenschutzrechtlichen Fragestellungen befassen, die mit Bonitätsanfragen in Verbindung stehen, bietet der Datenschutzblog „Datenschutzbeauftragter-Online“ eine gute Gelegenheit ihr Wissen zu erweitern.

Dort wird auf die Frage eingegangen, was unter Bonitätsanfragen zu verstehen ist, wie die Funktionsweise von Bonitätsanfragen aussieht sowie, ob Bonitätsanfragen vor dem Abschluss von Kaufverträgen gerechtfertigt sind. Abschließend erhält der Leser eine datenschutzrechtliche Bewertung der Problematik. Abgerundet werden die Informationen mit Hinweisen zum gleichen Thema, die bereits vom Düsseldorfer Kreis abgegeben wurden.

Quelle: [Datenschutzbeauftragter-Online](#)

Elena alarmiert Datenschützer

Ab dem 1. Januar 2010 müssen Arbeitgeber bundesweit die Einkommensdaten ihrer Beschäftigten verschlüsselt an eine zentrale Datenbank bei der Deutschen Rentenversicherung übertragen. Dort sollen diese pseudonymisiert abgelegt werden.

Ob Elena, der „Elektronische Entgelt-nachweis“ tatsächlich, die in sie gesetzten Hoffnungen als Mittel zum Bürokratieabbau und Katalysator für die Einführung einer digitalen Signatur erfüllen wird, oder sie sich als das ehemals von der FDP bezeichnete „Datenmonster“ entpuppen wird, muss sich noch zeigen.

Was Datenschützern bereits jetzt die

Sorgenfalten ins Gesicht treibt, ist die umfangreiche Datensatzbeschreibung, wonach Elena nicht nur wissen will, ob einem Arbeitnehmer z.B. wegen vertragswidrigem Verhaltens gekündigt wurde, sondern auch, worin dieses Verhalten bestand. Dafür ist ein Freitextfeld vorgesehen, welches vom Arbeitgeber mit Leben gefüllt werden soll. Wie kritisch Freitextfelder zu betrachten sind, wissen Datenschützer bereits aus dem Zusammenhang mit CRM-Systemen.

Auch Informationen über die Teilnahme an „rechtmäßigen bzw. unrechtmäßigen Streiks“ sollen eingetragen werden (können).

„Informationen zu Streiks hätten in einer solchen Datenbank nichts verloren“, so Peter Wedde von der Europäischen

Akademie der Arbeit der Uni Frankfurt. Der Datenschutzexperte mahnt zur Datensparsamkeit: „Gerade in diesen Zeiten des Datenmissbrauchs sollte der Staat seiner Vorbildfunktion gerecht werden und sparsam mit Daten umgehen“. Elena sei aber „weit übers Ziel hinausgeschossen“.

Der Arbeitskreis Vorratsdatenspeicherung rät allen Betroffenen, gegen die umfassende Datenspeicherung bei ELENA eine Verfassungsbeschwerde einzulegen. Und der Grünen-Politiker Spitz fordert: „Dieses Vorgehen muss schnellstmöglich auch durch ein eigenständiges Arbeitnehmerdatenschutzgesetz untersagt werden.“

Quellen: Heise.de und Zeit.de

Informationsschrift „Datenauswertung und personenbezogene Datenanalyse“

Die Datenschutzskandale der Vergangenheit haben die Datenauswertungen von Mitarbeitern in die Negativschlagzeilen der Medienlandschaft gebracht. Dabei wird bei der Berichterstattung außer Acht gelassen, dass die Analyse personenbezogener Daten die Revisionsarbeit seit Jahrzehnten begleitet.

Das deutsche Institut für Interne Revision e.V. (DIIR) hat in Kooperation mit der GDD eine Informationsschrift zu dieser Thematik erarbeitet. Sie wurde von einer Projektgruppe erstellt, an denen neben Vertretern des DIIR und GDD-Mitgliedern auch Herr Uwe Dieckmann, Vorstandsmitglied der GDD, beteiligt waren. Die Informationsschrift zeigt pragmatisch auf, wie einerseits personenbezogene Datenschutzinteressen andererseits auch Interessen der Unternehmen ausgewogen berücksichtigt werden können. Mit dieser Veröffentlichung wird dem Wunsch vieler Revisorinnen und Revisoren, aber auch Datenschutzbeauftragten Rechnung getragen, mehr praktische Hinweise für die Durchführung von automatisierten Datenanalysen und darüber hinaus gleichzeitig Leitlinie für die notwendige Beachtung regulatorischer Vorgaben im Zusammenhang mit der Analyse personenbezogener Daten zu erhalten.

Die Informationsschrift enthält deshalb neben einer detaillierten Darstellung möglicher Vorgehensweisen auch in einem eigenständigen Kapitel eine tabellarische Zusammenfassung unterschiedlicher Konstellationen bei der Datenanalyse mit einer Einordnung der Anwendbarkeit.

Die Informationsschrift des DIIR in Kooperation mit der GDD können Sie [hier](#) downloaden

Quelle: [Gesellschaft für Datenschutz und Datensicherung \(GDD e.V.\)](#)

