ISSN 2194-1025

AUSGABE 1/2013

BvD-News

Das Mitgliedermagazin

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

BvD-Infotag in Brüssel | ab Seite 6

Jan Philipp Albrecht im Interview | ab Seite 12

Datenschutztage am 24. und 25.04. | ab Seite 17

25 Jahre udis | ab Seite 27

BvD e.V.

Die Datenschützer

privacyGUARD

Strategischer Datenschutz mit privacyGUARD

Datenschutz muss im Vordergrund stehen,
aber im Hintergrund ablaufen.

- Analyse, Kontrolle, Optimierung und Dokumentation
- Zuarbeit durch Dritte (z.B. HTML-/Excel-Ex- und Import)
- Auftragsdatenverarbeitung, Mitarbeitersensibilisierung etc.

Vom Standardprodukt zu Ihrer Lösung

- Mehrmandantenfähig
- Modularer Aufbau (Konzern-Modul, Web-Oberfläche, Mehrsprachigkeit etc.)
- Individuelle Erweiterungen durch offene Schnittstellen

Spezielle Anforderungen bedürfen zielgerichteter Lösungen:
Wir beraten Sie gerne!

Eine kostenlose Demo-Version erhalten Sie unter
www.privacyguard.de/demo

otris software AG | Königswall 21 | D-44137 Dortmund | Fon +49 231 95 80 69 - 70 | privacyguard@otris.de

DATENSCHUTZ | SAP SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

eLearning Datenschutz

ein optimales Instrument zur Sensibilisierung und Schulung der Mitarbeiter

> Inhalte individuell anpassbar durch Content Management System

> Langjährige Aktualität durch Update Service

Bitte informieren Sie sich unter: http://www.ditis.de/eLearning_demo
Auch als eLearning Informationssicherheit erhältlich.

ditis Systeme – Niederlassung der JMV GmbH & Co. KG Heidenheim • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 13 • 89081 Ulm • Tel +49 731 509704 - 40 • E-Mail info@ditis.de • www.ditis.de

Editorial

Liebe Leser,
wer Datenschutz für bürokratischen Ballast hält, der ist nicht mehr von dieser Welt. Trotzdem tragen Lobbyisten verschiedener Bereiche in Brüssel genau diese überholte Aussage vor sich her und versuchen die Entwicklung hier aufzuhalten. Die Behauptung, Datenschutz verhindere Innovationen trifft ungefähr genauso zu, wie die Aussage, dass die Straßenverkehrsordnung die Weiterentwicklung des Automobils verhindert hat. Als erfahrene Praktiker wissen wir längst, dass die Verarbeitung von Daten heutzutage notwendig und unumkehrbar ist und dass diese nur durch klare Regeln ermöglicht werden kann. Insofern stellt das Verbot mit Erlaubnisvorbehalt eine zentrale Säule des Datenschutzes in Deutschland und hoffentlich auch in der kommenden EU-Datenschutzverordnung dar. Lebendiger innovativer Datenschutz sollte vielmehr zum Markenzeichen der EU werden.

Die Kunden erwarten dies in rasant zunehmendem Maße – und das nicht nur in der EU sondern auch in allen anderen Regionen der Welt. Daher ist die EU-DSGVO ein Modell, das schnell Schule machen wird, wenn es den Unternehmen in Europa den Marktvorteil eines guten Datenschutzniveaus bietet.

Der BvD begleitet das Verfahren zur Entwicklung einer EU-Datenschutzgrundverordnung mit verschiedenen Aktionen und Stellungnahmen und ist hier auch weiter aktiv.

An dieser Stelle möchte ich mich insbesondere bei Herrn Alexander Alvaro (dem Vizepräsident des EU-Parlaments) bedanken, der uns dabei unterstützt hat, die Parlamentarier in Brüssel vor Ort zu informieren. Aufgrund eines Autounfalles wird er nicht am BvD-Verbandstag teilnehmen können. Ich wünsche ihm alles Gute und weiter eine gute Genesung.

Auch auf dem Verbandstag werden wir umfassende Informationen zur EU-DSGVO anbieten und verschiedene Positionen dazu hören. Nutzen Sie die Gelegenheit, sich zu informieren oder gar den BvD bei seinen Aktionen zu unterstützen.
Viel Vergnügen mit der vorliegenden Ausgabe der BvD-News

Ihr Thomas Spaeing
BvD-Vorstandsvorsitzender

Inhaltsverzeichnis

- Editorial 3
- Lebhaftes Match um den Datenschutz von 500 Millionen Menschen 5
- EU-Parlamentarier bewerten BvD-Hinweise als wertvoll 6
- Aktuelle Entwicklungen zur EU-DSGVO 9
- „EU sollte Vorreiterin in Sachen Datenschutz werden“ 10
- Herausragende Sprecher bei den Datenschutztagen 17
- Der Steuerberater zwischen Funktionsübertragung und Auftragsdatenverarbeitung 20
- Mitstreiter für Datenschutz-Auskunftsportal gesucht 24
- 25 Jahre Ausbildung von Datenschutzbeauftragten 27
- Ulmer Resolution zum aktuellen Entwurf der EU-DSGVO 30
- Meilenstein für Datenträgervernichtung 31
- Es kommt, es kommt nicht, es kommt… oder vielleicht doch nicht? 35
- „Den meisten Menschen ist ihre Privatsphäre wichtig“ 36
- Datenschutz in der Arztpraxis – Thema für Aufsichtsbehörden? 38
- So wird der IT-Grundschutz-Standard implementiert 41
- Berechtigungen administrieren, dokumentieren und delegieren 46
- Aktuelle Meldungen ..... 48 & 72
- Erstmals mehr als 800 Mitglieder im BvD aktiv 50
- RG Süd wächst weiterhin sehr erfolgreich 51
- Mitglieder der RG Bayern diskutieren aktuelle Themen 52
- AK Externe informiert sich über die DATEV 53
- AK Medizin: Workshop zur Orientierungshilfe KIS 55
- AK Sozial etabliert sich 59
- AK Social Media – Ein Arbeitskreis stellt sich vor 60
- Evaluation von § 30a und § 42a BDSG durch Bundesregierung 61
- Datenschutz auf dem Social Learning Summit 13 64
- Datenschutz für Facebook-Nachrichten 66
- Arbeitnehmerdatenschutz beim Fleetmanagement 67
- Rezensionen 70
- Das Seminarangebot des BvD auf einen Blick 73
- Die Termine der RGs und AKs auf einen Blick 75

Impressum

BvD-News
Das Mitgliedermagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Herausgeber:
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Telefon (030) . 21 96 43 97
Telefax (030) . 21 96 43 92
E-Mail: bvd-gs@bvdnet.de
Internet: https://www.bvdnet.de

Redaktion: Thomas Spaeing (V.i.S.d.P., bvd-news@bvdnet.de) Jürgen Hartz, Rudi Kramer, Dr. Jens Eckhardt, Udo Wenzel, Stefan Staub, Thomas Floß, Claudia Seilert, Michael Braun

Fotos: Fotolia, Medienhaus Waltrop

Lektorat: Frank Spaeing

Produktion (Planung, Satz, Layout):
Medienhaus Waltrop, Dortmunder Straße 34-38, 45731 Waltrop, www.medienhaus-waltrop.de

Anzeigen:
Jürgen Hartz (juergen.hartz@bvdnet.de)

ISSN: 2194-1025

Erscheinungsweise: 3 x jährlich, ca. 2000 Exemplare

Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

Aufruf

Die Redaktion der BvD-News möchte in den kommenden Ausgaben externen Autoren noch mehr Platz einräumen. Wir sind interessiert an Meinungen, Stellungnahmen und Diskussionsanstößen, aber auch an Praxisberichten aus Ihrem Alltag im Umgang mit dem Datenschutz. Bei Interesse können Sie sich gerne an die Redaktion wenden und uns Ihr Thema vorschlagen. In den Redaktionskonferenzen diskutieren wir dann alle Texte und veröffentlichen sie je nach Thema und Relevanz in einer der folgenden Ausgaben. Schicken Sie Ihren Vorschlag, Ihre Idee oder Ihr Manuskript einfach per E-Mail an die Redaktionsadresse bvd-news@bvdnet.de. Wir freuen uns auf Ihre Beiträge!

Lebhaftes Match um den Datenschutz von 500 Millionen Menschen

Seit die EU-Kommission am 25. Januar 2012 die Vorlage ihres Reformpakets auf das Spielfeld der europäischen Politik kickte, hat sich ein durchaus lebhaftes Match entwickelt. Dabei geht es um nicht weniger als um den Datenschutz der mehr als 500 Millionen Europäerinnen und Europäer. Von dem Spielergebnis hängt aber nicht nur das zukünftige Datenschutzniveau in den 27 Mitgliedstaaten der Europäischen Union ab, sondern der Umgang mit personenbezogenen Daten in der globalen Informationsgesellschaft insgesamt. Denn genauso wenig wie sich digitale Daten an einem Ort festhalten lassen, beschränken sich die Auswirkungen des angepeilten Regelungswerks auf Europa. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in der vergangenen Woche daher erneut für die Stärkung des Datenschutzes auf europäischer Ebene eingesetzt.

Schon die Einführung des von der Kommission vorgeschlagenen und – jedenfalls in Europa – von niemandem ernsthaft in Frage gestellten Marktortprinzips kann Internet-Multis aus Übersee, die in Europa gute Geschäfte machen, nicht kalt lassen. Bisher haben sich einige der großen Internet-Unternehmen darauf berufen, für sie gelte europäisches Datenschutzrecht nicht. Zukünftig ist klar: Wer den europäischen Markt bedient und dabei die Daten europäischer Kundinnen und Kunden verarbeitet, muss sich an europäische Regeln halten. Damit stellt die Europäische Union einen Zustand her, wie er etwa im US-amerikanischen Recht seit eh und je gilt. Deshalb tue ich mich schwer, der von Vertretern amerikanischer Unternehmen vorgebrachten Kritik zu folgen, Europa würde damit das Territorialprinzip verletzen. Denselben Vorwurf müsste man dann auch US-amerikanischen Gerichten machen. Ohne Marktortprinzip würde das europäische Datenschutzrecht weitgehend leerlaufen, jedenfalls in Bezug auf Internet-Dienste.

Beklagt wird auch, dass die Aufsichtsbehörden nach dem Verordnungsentwurf hohe Bußgelder verhängen können – bis zu 2 % des Weltjahresumsatzes des Unternehmens, das gegen Datenschutzregeln verstößt. Diese Klage ist durchaus begründet, müssen doch bisher selbst Konzerne mit einem Umsatz in zweistelliger Milliardenhöhe nur mit Strafzahlungen von höchstens 300.000 Euro rechnen, wenn sie in Deutschland schwerste Datenschutzverstöße begangen haben. Ich finde es völlig richtig, dass auch große und finanzstarke Konzerne zukünftig nicht bloß ihre Portokasse bemühen müssen, wenn sie sich nicht an europäische Datenschutzregeln halten. Vielen Unternehmen ist das übrigens nicht unbekannt, denn die US-amerikanische Aufsichtsbehörde, die Federal Trade Commission, verfügt über mindestens gleichwertige Sanktionsbefugnisse. Auch wenn der maximale Strafrahmen nur in den seltensten Fällen ausgeschöpft werden dürfte, wird allein das Risiko empfindlicher Sanktionen zur Folge haben, dass unser Datenschutzrecht ernster genommen wird. Es ist zu hoffen, dass die europäischen Institutionen dem Druck von Lobbyisten widerstehen werden, den vorgesehenen Bußgeldrahmen einzuschränken.

Leider haben Drohgebärden und Lobby-Einflüsterungen in anderen Fragen bereits Wirkung gezeigt: So ist Entschließungsanträgen aus dem Europäischen Parlament zu entnehmen, dass ganze Wirtschaftsbereiche aus dem Anwendungsbereich des Datenschutzrechts ausgenommen werden sollen, etwa kleine Unternehmen. Auch Beschäftigtendaten sollen schutzlos gestellt werden. Interessant ist auch, dass wirtschaftsnahe Abgeordnete Daten mit beruflichem Hintergrund vom Geltungsbereich des Datenschutzes ausnehmen wollen. Ob ihnen eigentlich klar ist, dass dann sämtliche Informationen, die Freiberufler betreffen, etwa zu ihrem Einkommen, frei zugänglich würden? Der Vorschlag, nur noch solche Daten als personenbezogen anzusehen, die von den jeweiligen Unternehmen oder staatlichen Stellen selbst namentlich zugeordnet werden können, ist ein trojanisches Pferd US-amerikanischer Internetkonzerne. Internetkonzerne könnten sich aus den Vorgaben des Datenschutzrechts herausstehlen, in dem sich darauf berufen, nicht zu wissen, welche Person hinter einer IP-Adresse oder einer Cookie-ID steht.

Es ist zu hoffen, dass die Weichmacher, die das EU-Datenschutzrecht sogar weit unter das seit 1995 bestehende Niveau drücken wollen, keine mehrheitliche Unterstützung bei den europäischen Gremien finden. Das Europäische Parlament und der Rat der Europäischen Union haben die Chance, den Verfassungsauftrag zum Schutz personenbezogener Daten mit Leben zu füllen. Es ist zu hoffen, dass sie diese Chance nicht verstreichen lassen, wenn sie am Ende der ersten Halbzeit des Gesetzgebungsprozesses ihre jeweiligen Stellungnahmen abgeben.

Entschieden wird das Spiel in der zweiten Halbzeit, im sogenannten Trilog, in dem sich Parlament, Rat und Kommission bis Anfang 2014 verständigen müssen. Es bleibt also spannend!

Autor

Peter Schaar
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

(Quelle: BfDI)

EU-Parlamentarier bewerten BvD-Hinweise als wertvoll

Infoveranstaltung des Verbandes in Brüssel mit guter Resonanz, interessanten Gesprächen und wichtigen Kontakten

BvD-Vorsitzender Thomas Spaeing eröffnete gemeinsam mit Alexander Alvaro die Infoveranstaltung in Brüssel.

Eine Vereinheitlichung des europäischen Datenschutzes ist überfällig. In zu vielen Ausprägungen wurden in den Mitgliedsstaaten die Richtlinie von 1995 umgesetzt. Die einzelnen Ausprägungen des Entwurfs einer Datenschutzgrundverordnung (EU-DSGVO-E) der Europäischen Kommission vom 25. Januar 2012 skizzierte BvD-Vorstand Dr. Jens Eckhardt bereits in der BvD-News 1/2012. Dabei werden fast alle Bereiche neu geregelt, nicht nur die, welche durch die technischen Entwicklungen der letzten 20 Jahre betroffen sind. Nicht vergessen werden darf hierbei die Tatsache, dass wir in der Regel immer nur das BDSG im Hinterkopf haben, die Kommission aber die rechtlichen Hintergründe von 26 weiteren Mitgliedstaaten im Blick haben muss. Umso erfreulicher ist es, dass das deutsche Modell des Datenschutzbeauftragten als Vorbild dient. Doch nicht nur in diesem Bereich, auch bei anderen Regelungen innerhalb des Entwurfs der Kommission blieben die Formulierungen hinter den Anforderungen der Praxis zurück. Die Folge sind zumindest Unklarheiten in der Auslegung bis hin zur Rechtsunsicherheit für die Beratung der Unternehmen und Verlust einer Planungssicherheit über Jahre hinaus, bis sich durch Aufsichtsbehörden und Rechtsprechung in vielen Bereichen eine belastbare Rechtsmeinung gebildet hätte.

Der BvD entschloss sich deshalb, eine eigene Stellungnahme zu veröffentlichen, die als Positionspapier im Oktober an die EU-Parlamentarier und an die Kommission versandt wurden. Hierin wurden

neben der Hervorhebung der Beibehaltung des Verbots mit Erlaubnisvorbehalt sieben Hinweise formuliert (in kursiv die Artikel aus dem Entwurf der EU-DSGVO in der Fassung des Berichterstatters Albrecht vom 10.01.2013),

- den Anwendungsbereich der EU-DSGVO (Erwägungsgrund 23 hinsichtlich anonymer Daten)
- die Verwendung der Pseudonymisierung (Art. 4 Abs. 2a EU-DSGVO-E)
- die Stellung und Aufgaben eines DSB (Erwägungsgrund 75a (neu); Art. 34 Abs. 2; Art. 35 Abs.1; Art. 35 Abs. 7; Art 35 Abs. 11; Art. 36 Abs. 3; Art. 36 Abs. 3a; Art. 22 Abs. 2 lit d EU-DSGVO-E)
- die Klärung der Verantwortlichkeit bei einer Verarbeitung im Auftrag
- die Gleichstellung von Sozialdaten mit Gesundheitsdaten (Art. 82a EU-DSGVO-E)
- die Informationspflicht bei Datenpannen (Security Breach Notification) (Art. 32 Abs. 1 EU-DSGVO-E)
- und das Verhältnis zu Rechtsvorschriften in Mitgliedsländern zu berufsrechtlichen Verschwiegenheitsverpflichtungen betreffen (Art. 84 Abs. 4 EU-DSGVO-E).

Darstellungen aus der Praxis bei Parlamentariern sehr willkommen

In der Folge dieses Positionspapiers fanden Gespräche mit unterschiedlichen Stellen aus dem Umfeld des Gesetzgebungsverfahrens statt, um sich über die Positionen auszutauschen. Darüber hinaus fand Ende November auf Einladung von Alexander Alvaro, Mitglied im Ausschuss LIBE (Bürgerliche Freiheiten, Justiz und Inneres) und Schattenberichterstatter zur EU-DSGVO-E, eine Informationsveranstaltung in Brüssel statt, um die Mitglieder des europäischen Parlaments (MdEP) über die Aufgaben

Die EU-Parlamentarier zeigten sich sehr interessiert und fragten intensiv nach.

Prof. Dr. Rolf Schwartmann gab in der BvD-Veranstaltung für die GDD eine Stellungnahme in Brüssel ab.

eines DSB zu informieren und die Vorteile und Entlastungen für die Unternehmen darzustellen.

Unter dem Titel „Der Datenschutzbeauftragte in Europa - Besserer Datenschutz – weniger Bürokratie" fanden sich MdEPs und interessierte Mitglieder in einem Sitzungsraum des Europäischen Parlaments ein, um sich direkt von Datenschutzbeauftragten informieren zu lassen. Nach der Begrüßung und Vorstellung der Referenten durch den BvD-Vorsitzenden Thomas Spaeing betonte der Gastgeber Alexander Alvaro, dass die Größe eines Unternehmens keine nachvollziehbare Grenze für einen effektiven Datenschutz sein könne. Nachdem Thomas Spaeing die Grundzüge der Gestaltung der DSB-Stellung und Aufgaben im BDSG vorstellte, erläuterte Prof. Dr. Rolf Schwartmann als Vorsitzender der GDD kurz die Hintergründe und Möglichkeiten von delegierten Rechtsakten, kritisierte deren Anzahl im Entwurf der Kommission und regte u.a. an, die Bestellpflicht eines DSB bei 50 Mitarbeitern anzusetzen.

Beispiele und Erwartungen aktiver DSBs: Danach wurde durch Nikolaus Schenk, DSB an den Kliniken des Bezirks Oberbayern, die Tätigkeit eines DSB im medizinischen Umfeld sowie die Einbeziehung europäischer Datenschutzregelungen durch die Nähe zu Österreich erläutert. Er sieht in der Fassung der EU-DSGVO der Kommission künftig die Schwierigkeit bei einer Bestellpflicht ab 250 Mitarbeitern bei vielen Lieferanten keinen fachkundigen Ansprechpartner für datenschutz-

Rudolf Berthold Gerhard und Chris Newiger stellten zentrale Fragen des Datenschutzes jeweils aus ihrer fachlichen Sicht dar. (Fotos: Michael Braun)

rechtliche Anforderungen mehr zu haben. Die Sichtweise eines RZ-Dienstleisters legte Rudolf Berthold Gerhard, DSB bei der DATEV eG, dar. Für ihn fördert ein DSB das Vertrauen der Kunden und Betroffenen in die Datenverarbeitung. In seinem Vortrag wies er auf die Aspekte hin, dass der Schutz von Berufsgeheimnissen gewahrt bleibt und der Dokumentationsaufwand bei Auftragsverarbeitung reduziert wird.

Ebenso wichtig waren ihm die Möglichkeit der Selbstregulierung und die Einführung von Verfahren zur Freigabe von Corporate Rules, sowie auf die wesentliche Grundsätze für einen effektiven DSB hinzuweisen. Als DSB eines multinationalen Konzerns (Deutsche Bahn AG) beschränkte sich Chris Newiger nicht nur darauf, ihr Aufgabengebiet und die weltweit – schier unübersichtlichen – rechtlichen Grundlagen darzustellen. Sie hielt auch ein engagiertes Plädoyer, dem DSB die Rückendeckung zu geben, die er braucht, um die Interessen der Betroffenen wahrzunehmen, das Unternehmen objektiv weisungsfrei zu beraten und das Vertrauen, das Betroffene und Unternehmensleitung in ihn setzen, zu rechtfertigen. Hierfür sei eine gesetzliche Verschwiegenheitsregelung zugunsten der Betroffenen für den DSB unerlässlich.

Abschließend erläuterte Thomas Spaeing u.a., dass die Einführung eines DSB bei vielen Unternehmen auch durch einen externen DSB geregelt werden kann, der – sofern die Grundlagen geregelt sind und der Unternehmenzweck nicht in der Verarbeitung von Daten besteht, auch mit wenigen Beratungstagen auskommen kann. Zum Schluss der Veranstaltung resümierte Jan Philipp Albrecht, der Berichterstatter des Ausschusses LIBE, dass er wertvolle Hinweise und Details mitnehme und in der weiteren Diskussion berücksichtigen werde. Die Position des DSB sei bei der Mehrheit der MEdP positiv aufgenommen worden.

Wie geht es weiter? Der Bericht von Jan Philipp Albrecht wurde am 10.Januar 2013 veröffentlicht. Das Europäische Gesetzgebungsverfahren sieht vor, dass sich Parlament, Ministerrat und Kommission einig sein müssen – siehe auch das Interview zu seinem Bericht mit Jan Phillip Albrecht in diesem Heft.

Hinweis am Ende: Der Entwurf der Kommission vom 25. Januar 2012, die Stellungnahme des BvD vom 18. Oktober 2012, die Folien der Referenten und der Videostream der Veranstaltung vom 27. November 2012 sowie der Bericht des Berichterstatters Albrecht sind auf der BvD-Homepage veröffentlicht.

Die Veranstaltung wurde live im Netz übertragen. Nikolaus Schenk (unten) berichtete aus seiner Praxis.

Aktuelle Entwicklungen zur EU-DSGVO

Was macht der Rat bei der EU-Datenschutzgrundverordnung?

Was immer die EU-Kommission auch vorschlägt: bei der EU-DSGVO müssen sich letztendlich drei europäische Einrichtungen einigen: Neben dem EU-Parlament gehört auch der Ministerrat dazu, der sich aus den Vertretern der europäischen Mitgliedsstaaten, in der Regel den zuständigen Fachministern, zusammensetzt. Die Bundesrepublik Deutschland wird daher im Rat bei der EU-DSGVO durch den Bundesinnenminister vertreten.

Die Vorstellungen einzelner Parlamentarier und deren Ausschüsse sind sehr transparent dargestellt. Die Meinungsbildung im Ministerrat verläuft dagegen nicht öffentlich, müssen sich doch 27 Länder erst intern verständigen.

Der Entwurf der Kommission wurde im Rat zunächst chronologisch durchgearbeitet, um dabei schon die unterschiedlichen Positionen und Ansichten auszutauschen. Man darf auch nicht vergessen, dass etliche Staaten der Europäischen Union aufgrund der knappen finanziellen Mittel die Einrichtung von Aufsichtsbehörden, aufwändigen internationalen Kohärenzverfahren zur Abstimmung von Einzelfragen und mögliche Übersetzungskosten etc. nicht begeistert aufnehmen. Die Finanzkrise trägt mit knappen Kassen das ihre dazu bei.

Risikobasierter Ansatz: Anfang März wurden im Rahmen der Beratungen des Rates der Europäischen Union in einer Mitteilung über den Stand der Meinungsbildung berichtet (http://register.consilium.europa.eu/pdf/en/13/st06/st06607-re01.en13.pdf). Danach unterstützen die Mitgliedsstaaten die Fortführung eines risikobasierten Ansatzes. Dies ist in schöner Tradition der grundlegenden Festlegungen in der Richtlinie von 1995 dass schon jetzt risikoreichere Informationen hinsichtlich einer Persönlichkeitsverletzung nach dem Willen des Gesetzgebers anders behandelt werden. Ob dies auch dem Rat ausreicht, ist derzeit noch offen: unter einem risikobasierendem Ansatz ließe sich selbst eine Abkehr des Grundsatzes des Verbots mit Erlaubnisvorbehalt darstellen. Lassen wir uns überraschen, was der Rat und das Bundesinnenministerium in einem Wahljahr darunter tatsächlich verstehen.
Datenschutzbeauftragter: Überlegungen im Ministerrat, auch bei der Bestellpflicht des Datenschutzbeauftragten den risikobasierenden Ansatz zu betonen, vernachlässigen die praxisnahe Konstellation, dass jedes personenbezogene Datum relevant sein kann und das auch scheinbar harmlose Daten in Kombination zu einer Risikosituation führen können. Hier sind die bisherigen Äußerungen seitens der Parlamentarier und der Kommission beachtenswert, die am Verbot mit Erlaubnisvorbehalt festhalten.

Selbstregulierung: Ein weiterer interessanter Aspekt betrifft die Selbstregulierung, die der Rat stärker verankert haben möchte. Obwohl dies bereits in § 38a BDSG im Kern angelegt ist, gibt es dennoch kaum Umsetzungen in Deutschland: Hier könnten in der EU-DSGVO Verbesserungen eingeführt werden, welche die Anforderungen und Prozesse zur Einrichtung, zu den Vorteilen (die daraus erwachsen können) sowie zu den Konsequenzen (die sich aus einer Nichteinhaltung ergeben), regeln. Dabei ist den Beteiligten hoffentlich bewusst, dass es dabei nicht um die Begründung von Zulässigkeitstatbeständen gehen kann. Letztendlich ist es begrüßenswert, wenn es Regelungen gibt, die Lücken schließen können, sollte der Gesetzgeber nicht in der Lage sein, Standards zu definieren, wie beispielsweise beim Datenschutzauditgesetz.

Flexibilität für den öffentlichen Bereich: Irritierend erscheinen die Überlegungen, dem öffentlichen Sektor besondere Flexibilität zuzugestehen, um das Datenschutzrecht den besonderen Anforderungen an den öffentlichen Bereich bzw. an die verfassungsrechtlichen Hintergründe der Mitgliedsstaaten anzupassen. Dies lässt außer Acht, dass gerade hier die betroffene Person in der Regel kein Wahlrecht hat, wer seine Daten beispielsweise durch Vertrag oder Einwilligung erheben darf. Gerade dann sind Regelungen erforderlich, die den Anschein vermeiden, der öffentliche Bereich hätte hier eine beliebige Gestaltungsmöglichkeit.

Wir werden die Entwicklungen weiter beobachten und die Vorteile und Erfahrungen des deutschen Datenschutzmodells hervorheben.

„EU sollte Vorreiterin in Sachen Datenschutz werden“

Jan Philipp Albrecht, Berichterstatter im EU-Parlament, im Interview mit den BvD-Vorständen Dr. Jens Eckhardt und Rudi Kramer

Grünen-Politiker Jan Philipp Albrecht ist Berichterstatter des Ausschusses LIBE im Europäischen Parlament. (Foto: Fritz Schumann)

Nach dem Entwurf der EU-Kommission zu einer Reform des europäischen Datenschutzrechts durch eine EU-Datenschutz-Grundverordnung (EU-DSGVO-E) vom 25.1.2012 ist das EU-Parlament am Zuge. Im zuständigen Ausschuss LIBE (Bürgerliche Freiheiten, Justiz und Inneres) koordiniert Jan Philipp Albrecht (Grüne) als Berichterstatter des Ausschusses die Meinungsbildung. Er legte am 10.1.2013 seinen Bericht vor. Mit ihm sprachen Dr. Jens Eckhardt und Rudi Kramer vor allem über die zukünftige Rolle des betrieblichen Datenschutzbeauftragten, weitere wesentliche Einzelaspekte des Berichts und das weitere Gesetzgebungsverfahren der EU-DSGVO.

BvD: Welchen Stellenwert hat für das EU-Parlament die Datenschutz-Grundverordnung?

Philipp Albrecht: Die Kommission hat mit der Erarbeitung eines Entwurfs dem Wunsch des Parlaments entsprochen, das europäische Datenschutzrecht an technische Entwicklungen anzupassen und eine einheitliche Rechtslage in Europa herzustellen. Das Gesetzesvorhaben ist für viele Parlamentarier das wichtigste Vorhaben in der Legislaturperiode: Es regelt die Datenschutzrechte aller Bürgerinnen und Bürger der EU und wirkt sich unmittelbar auf alle Unternehmen in der EU aus – aber auch auf Unternehmen, die ihren Sitz nicht in der EU haben, aber ihre Leistungen gegenüber EU-Bürgern anbieten. Die EU-DSGVO wird für die nächsten Jahre die Maßstäbe setzen, die benötigt

werden, um Grundrechtsschutz und wirtschaftliche Entwicklung in einer digitalisierten Welt zu garantieren.

„Das Gesetzesvorhaben ist für viele Parlamentarier das wichtigste Vorhaben in der Legislaturperiode“

BvD: Während des Gesetzgebungsverfahrens wurde durch Parlamentarier die Unterstützung durch Datenschutzorganisationen eingefordert, um ein inhaltlich argumentatives Gegengewicht gegenüber einseitig nur auf wirtschaftliche Interessen gerichteten Lobbyismus zu bilden. Hat der Appell gefruchtet und welche Unterstützung wurde trotzdem vermisst?

Albrecht: Zunächst hatte man den Eindruck, dass die Bestrebungen der Kommission nur seitens großer Unternehmen, die im Bereich Werbung und Internetdienstleistungen aktiv sind, wahrgenommen werden. Doch dann interessierten sich auch andere Branchen und auch Verbraucherorganisationen für die Inhalte. Von den Datenschutzverbänden kamen zunehmend praxisnahe Anregungen, die bei der Beurteilung des Berichts der Kommission bewertet wurden.

BvD: Welchen Einfluss haben Stellungnahmen und Aktionen – wie bspw. die Stellungnahme des BvD vom 18.10.2012 und die Informationsveranstaltung am 27.11.2012 in Brüssel – für die Meinungsbildung bei Parlamentariern? (Anmerkung: Die Hinweise des BvD in seiner Stellungnahme vom 18.10.2012 betrafen: Anwendungsbereich der EU-DSGVO-E (Personenbezug); Pseudonymisierung; Datenschutzbeauftragter (Fachkunde, Weiterbildung, Kündigungsschutz); Verantwortlichkeit bei Verarbeitung im Auftrag; Schutz von Sozialdaten; Bagatellklausel bei Security Breach Notification)

Albrecht: Gerade die Hinweise aus Praktikersicht halfen, die Überlegungen seitens der Kommission und auch von Parlamentariern aus dem Blickwinkel der Anwender zu beurteilen. So konnten beispielsweise Anregungen zur Verschwiegenheit oder zur Unabhängigkeit des Datenschutzbeauftragten (DSB), aber auch materiell-rechtliche Anmerkungen wie der Schutz von Sozialdaten oder Sonderregelungen bei Berufen, die einem Berufsgeheimnis unterliegen, nach einer Bewertung angemessen berücksichtigt werden. Die sachbezogene Expertise unterstützte bei der Meinungsbildung

In der BvD-Infoveranstaltung in Brüssel ergriff Albrecht das Wort und hob hervor, wie wichtig den EU-Parlamentariern der Input durch externe Fachleute ist.

über die Vorteile eines Datenschutzbeauftragten, wenn einige Grundregeln beachtet werden, wie die Fachkundeanforderung in dieser Position.

BvD: Durch die EU-DSGVO-E wird die Einrichtung eines Datenschutzbeauftragten europaweit eingeführt. Wie wurde die Einführung eines DSB bei Parlamentariern aufgenommen, die diese Position bisher nicht kannten?

Albrecht: Die Parlamentarier waren durchweg interessiert, wie die Einbeziehung eines Experten in die Beratung bei dem Umgang mit personenbezogenen Daten gelingt, ohne einen Verwaltungsapparat dafür einzurichten. Hier überzeugte die Möglichkeit, auch einen externen Datenschutzbeauftragten zu bestellen. Denn er kann das Unternehmen fachkundig beraten, während die Kosten im Rahmen bleiben.

„Bei frühzeitiger Einbeziehung ist jeder Datenschutzbeauftragte ein Gewinn für die Planungssicherheit und das regelkonforme Verhalten von Unternehmen“

BvD: Was ist nach Ihrer Einschätzung einfacher zu formulieren: die Voraussetzungen, wann Unternehmen einen Datenschutzbeauftragten benötigen oder wann nicht?

Albrecht: Ganz eindeutig: die Voraussetzungen, wann ein Datenschutzbeauftragter zu bestellen ist. Die Regelungen sind jetzt so klar formuliert,

Im Gespräch mit BvD-Vorstand Rudi Kramer nahm Jan Philipp Albrecht ausführlich Stellung zum Gesetzgebungsverfahren. (Fotos: Michael Braun)

dass jede Unternehmensleitung selbst einschätzen kann, ob die Voraussetzungen nach Art. 35 Abs. 1 EU-DSGVO-E vorliegen. Es wird über die Regelung in Art. 35 Abs. 9 EU-DSGVO-E sichergestellt, dass die Entscheidung der Unternehmensleitung in jedem Fall dokumentiert wird.

BvD: Welche Anreize gibt es für Unternehmen, einen Datenschutzbeauftragten zu bestellen, auch wenn es keinen bräuchte – also kein Fall einer Pflichtbestellung gegeben ist?

Albrecht: Die Unternehmen entlasten sich formell von Kontakten mit den Aufsichtsbehörden, wenn sie durch den Datenschutzbeauftragten fachkundig bestimmte Einschätzungen selbst durchführen können, ohne mit einer Aufsichtsbehörde in Kontakt treten zu müssen wie in Art. 34 Abs. 2 EU-DSGVO-E (Anmerkung der Redaktion: Art. 34 Abs. 2 EU-DSGVO-E regelt, dass statt der Aufsichtsbehörde auch der Datenschutzbeauftragte bei einer Datenschutzfolgeabschätzung mit bestimmten hohen Risiken zu Rate gezogen werden kann). Zudem darf der Vorteil eines direkten Ansprechpartners, der das Unternehmen und die Branche kennt, nicht unterschätzt werden. Bei frühzeitiger Einbeziehung ist jeder Datenschutzbeauftragte ein Gewinn für die Planungssicherheit und das regelkonforme Verhalten von Unternehmen. Datenschutzkonformes Verhalten ist mehr eine Reputationsfrage geworden, als die Frage nach der Vermeidung von Bußgeldern – auch hier kann eine fachkundige Beratung Beeinträchtigungen für das Unternehmen vermeiden helfen.

BvD: Reichen als Grundlage für die Erwartungen an die Fachkunde des Datenschutzbeauftragten die Ausführungen in den Erwägungsgründen (Erwägung 75a neu)? Die Festlegung der Details wird dem Europäischen Datenschutzausschuss übertragen (Art. 35 Abs. 11 EU-DSGVO-E).

Albrecht: Wir haben bewusst nur in den Erwägungsgründen der Verordnung die Anforderungen an die Fachkunde konkretisiert. Der Europäische Datenschutzausschuss hat eher die Möglichkeit, auf technische und rechtliche Änderungen der fachlichen Anforderungen zu reagieren. Ziel muss sein, dass der Datenschutzbeauftragte die Unternehmensleitung so beraten kann, dass diese frühzeitig Risiken und Möglichkeiten bei der Verarbeitung von personenbezogenen Daten erkennen und danach handeln kann.

BvD: Ihr Entwurf erweitert die Fassung der Kommission um eine Verschwiegenheitsverpflichtung des Datenschutzbeauftragten. Welche Änderungen bei der Rechtsstellung des Datenschutzbeauftragten gab es noch?

Albrecht: Wir haben die Mindestbestelldauer von zwei auf vier Jahre verdoppelt, damit die Unabhängigkeit des Datenschutzbeauftragten betont, aber auch eine qualifizierte Beratung außerhalb der Einarbeitungszeit sichergestellt wird. Um seiner Aufgabe effektiv nachkommen zu können, sieht die Verordnung vor, dass der Datenschutzbeauf-

Dr. Jens Eckhardt führte als BvD-Vorstand gemeinsam mit Rudi Kramer das Interview.

tragte Unterstützung hinsichtlich der benötigten Mittel beanspruchen kann. Er wird direkt der Unternehmensleitung unterstellt (Art. 36 Abs. 2 EU-DSGVO-E) und hat nun nicht nur eine Vertraulichkeitsverpflichtung, sondern in Einzelfällen auch ein Zeugnisverweigerungsrecht nach Art. 36 Abs. 3a EUDSGVO-E.
In diesem Kontext ist auch anzusprechen, dass nach unserer Konzeption der bestellte Datenschutzbeauftragte kraft Verordnung nur auf die Einhaltung des Datenschutzes hinwirken muss, die Verantwortung für die (Nicht-)Einhaltung bleibt hingegen bei dem für die Verarbeitung Verantwortlichen – also dem Unternehmen selbst.
Darüber hinaus wird die Stellung des betrieblichen Datenschutzbeauftragten im Unternehmen durch meinen Vorschlag insgesamt gestärkt. Er soll beispielsweise der Geschäftsleitung direkt unterstellt sein und die Mindestdauer seiner Bestellung wird verlängert, damit er effektiver auf die Einhaltung des Datenschutzes hinwirken kann.

BvD: Die Erwägungsgründe 23 und 24 sowie die Definition „betroffene Person" wird im Vorschlag überarbeitet, um den Anwendungsbereich des Datenschutzrechts zu konkretisieren. Folgt die EU-DSGVO-E damit dem objektiven oder dem relativen Ansatz zur Bestimmung des Personenbezugs? IP-Adressen von Unternehmen sollen den Anwendungsbereich nicht eröffnen. Wie stellen Sie sich die Abgrenzung zu anderen personenbeziehbaren Daten in der Praxis (z.B. Nutzung von Google Analytics) vor?
Albrecht: Entscheidend ist zunächst, dass die Abgrenzung zur Anonymisierung und die Definition der Pseudonymisierung mit dem Vorschlag in die EU-DSGVO-E aufgenommen werden, um den Anwendungsbereich zu konkretisieren. Bei der Definition des Personenbezugs soll deutlich werden, dass entscheidend ist, ob der Zusammenhang zwischen Information und Person mit angemessenen Mitteln hergestellt werden kann. Der Personenbezug kann daher variieren, ist aber vor allem zukunftsoffenen, um neue technische Entwicklungen der Personalisierung zu erfassen.
Am Beispiel der dynamischen IP-Adresse lässt sich das verbildlichen: Die dynamische IP-Adresse (IPv4) ist nicht zwingend und stets personenbezogen. Wenn der für die Verarbeitung Verantwortliche zur IP-Adresse so viele Informationen (gesammelt) hat, dass ein Individuum identifizierbar und durch ihn ansprechbar ist, dann ist ein Personenbezug gegeben. Entsprechend wird sich die Personenbeziehbarkeit der dynamischen IP-Adresse durch den Wechsel von IPv4 zu IPv6 ändern.
Mit der Definition der pseudonymisierten Daten soll der Anreiz zur Pseudonymisierung insbesondere in der Online-Umgebung gesteigert werden.
Bei der Verwendung anonymer Daten ist die EU-DSGVO-E nicht anwendbar. Pseudonymisierte Daten unterfallen hingegen weiterhin dem Datenschutzrecht und der EU-DSGVO-E. Der Schutz des Datenschutzrechts soll auf Menschen – rechtlich formuliert: natürliche Personen – beschränkt bleiben. Daten über „Unternehmen" fallen daher nicht in den Anwendungsbereich der EU-DSGVO-

Jan Philipp Albrecht tauscht sich intensiv mit Alexander Alvaro, dem Vizepräsidenten des Europäischen Parlamentes, aus.

E. Mit Unternehmen sind juristische Personen (GmbH, AG, etc.) gemeint. Lässt sich aber bei der Verarbeitung personenbezogener Daten nicht zwischen Daten über juristische und natürliche Personen differenzieren (beispielsweise IP-Adressen von Unternehmen und Verbrauchern beim Einsatz von Reichweitenmessungen). dann ist für die Anwendung des Datenschutzrechts entscheidend, dass zumindest auch Daten natürlicher Personen verarbeitet werden – sofern diese Daten einer Person zugeordnet werden können und damit personenbezogene Daten sind.

BvD: Dem Kommissionsentwurf wurde vorgehalten, zu wenig materiell-rechtliche

Zulässigkeitstatbestände zu regeln. Regelt nun Art. 6 Abs. 1b c) EU-DSGVO-E für Zwecke der Werbung die Zulässigkeit abschließend? Warum wurden keine eigenen weiteren Zulässigkeitstatbestände wie z.B. für Videoüberwachung etc. geschaffen?

Albrecht: Die Verordnung regelt nur die Sachverhalte abschließend, die in der Verordnung erwähnt sind. So gibt die Regelungen über die Erhebung von Daten für Zwecke der Werbung für die Mitgliedsstaaten keine Möglichkeit, eigene Zulässigkeitstatbestände zu definieren. Die EU-DSGVO-E regelt den Sachverhalt der Werbung in Art 6 Abs. 1b lit c EU-DSGVO-E und somit abschließend.

Anders bei der Videoüberwachung: hierzu ist in der VO nichts geregelt. Die Mitgliedstaaten können hier eigene Regelungen zur Erhebung schaffen. Öffentliche Stellen unterliegen dabei dem Gesetzesvorbehalt, da hier Art. 6 Abs. 1a Satz 4 EU-DSGVO-E als Zulässigkeitsgrundlage der Interessensabwägung nicht gilt.

BvD: Und Videoüberwachung durch Unternehmen?

Albrecht: Sofern die Mitgliedstaaten von ihrer Gestaltungsmöglichkeit keinen Gebrauch machen und Erhebungstatbestände schaffen, können Unternehmen unter ordnungsgemäßer Abwägung der Interessen nach Art 6 EU-DSGVO-E Videoüberwachung vornehmen.

BvD-Vorstandsvorsitzender Thomas Spaeing im Gespräch mit Jan Philipp Albrecht.

Das vitale Interesse der für die Verarbeitung Verantwortlichen sehe ich dabei beispielsweise auch bereits beim Eigentumsschutz an. Natürlich birgt dies die Gefahr, dass die Mitgliedstaaten dabei ihre bisherige Rechtsauffassung hineininterpretieren. Doch die Grundlagen der Berücksichtigung der berechtigten Interessen, wie sie aktuell durch das BDSG und die Auslegung der Aufsichtsbehörden umgesetzt wird, wie Kennzeichnungspflicht, und Datenminimierung sowie die Zweckbindung dienen auch nach der VO dazu, die Interessen der betroffenen Personen zu schützen.

Wichtig ist dabei, herauszustellen, dass dieser Spielraum für die Mitgliedstaaten allein bei der Erhebung personenbezogener Daten besteht. Die Verarbeitung personenbezogener Daten regelt die EUDSGVO-E abschließend.

BvD: Sollte nun die Bundesregierung im BDSG noch durch eine Änderung des Beschäftigtendatenschutzes Zulässigkeitstatbestände für die Videoüberwachung regeln, so…?

Albrecht:... so gelten diese auch nach Inkrafttreten der EU-DSGVO-E (nach dem aktuellen Stand) weiter.

BvD: Im Fall des Art. 31 und 32 EU-DSGVO-E („Security Breach Notification") sehen Sie in den Erwägungsgründen eine Änderung vor (Änderungsantrag 45 zu Erwägungsgrund 67: Meldefristverlängerung und Verhältnismäßigkeitserwägungen). In der Verordnung findet sich die Verhältnismäßigkeit dann aber nur bei der Informationspflicht gegenüber den betroffenen Personen wieder.

Albrecht: Zunächst sind durch einen redaktionellen Fehler in der Fassung vom 10. Januar die Änderungen bei Art. 31 und 32 nicht vollständig in der Verordnung wiedergegeben worden. Dieser formelle Fauxpax seitens der Sekretariate wurde noch am 10. Januar durch ein Erratum – eine Korrekturergänzung zum Bericht – klargestellt. Wir gehen dabei davon aus, dass es genügt, dass die Aufsichtsbehörden in jedem Fall informiert werden und die betroffenen Personen nur, wenn nach Ablauf der Meldefrist eine Datensicherheitsverletzung nicht auszuschließen ist.

BvD: Werden dann die Aufsichtsbehörden nicht durch zu viele unnötige Meldungen

von der wichtigeren Arbeit abgehalten?
Albrecht: Die Meldefristverlängerung soll diesem Bedenken Rechnung tragen. Oftmals können Unstimmigkeiten schnell ausgeräumt werden und belasten damit nicht die Aufsichtsbehörden. Für die dann noch eingehenden Meldungen werden sich die Aufsichtsbehörden so organisieren, dass sie mit dem Aufkommen gut umgehen können.

BvD: Welche Überlegungen führten zu einer Formulierungsänderung bei Art. 84 von „Grenzen dieser Verordnung" (Kommissionsentwurf) hin zu „in Übereinstimmung mit den Bestimmungen dieser Verordnung" in Ihrem Bericht?
Albrecht: Diese Formulierung erfolgte nur zur Klarstellung, bevor Interpretationen unterstellen, „im Rahmen" erlaube auch ein „Nicht-Erreichen" der in der VO getroffenen Vorgaben.

Der EU-Berichterstatter verfolgte gemeinsam mit Rudi Kramer die Ausführungen der Experten auf dem BvD-Infotag in Brüssel.

BvD: In Ihrem Bericht werden statt der Kommission in delegierten Rechtsakten nun dem Europäischen Datenschutzausschuss (bisherige Art. 29 Gruppe) verstärkte Entscheidungskompetenzen eingeräumt, z.B. bei der Festlegung der Qualifikation eines Datenschutzbeauftragten in Art. 35 Abs. 11 EU-DSGVO-E. Warum wird in der EU-DSGVO-E hierzu keine inhaltliche Aussage getroffen und traut man der Kommission hierzu keine Kompetenz zu?
Albrecht: Der Europäische Datenschutzausschuss trifft keine Entscheidungen im Sinne gesetzlicher Vorgaben, sondern bindet sich lediglich selber. Hinweise, dass auch der Europäische Datenschutzausschuss nicht demokratisch legitimiert sei, gehen somit ins Leere. Er ist aber fachkompetent und sachgebietsnah, um in den ihm zugewiesenen Fällen zu beraten oder Vorgaben zu erstellen.

BvD: Wie wird die Planungssicherheit für Unternehmen gewährleistet, wenn es für die EU-DSGVO-E eine Übergangsfrist von 2 Jahren geben soll, aber unklar ist, wann wesentliche inhaltliche Vorgaben durch Kommission oder Europäischen Datenschutzausschuss kommen? (Vgl. Art. 23 Abs.3 EU-DSGVO-E: Vorgaben zu datenschutzfreundlicher Technik)
Albrecht: Die Kommission ist über die Verordnung angehalten, die ihr per delegiertem Rechtsakt übertragenen Aufgaben vor Inkrafttreten der Wirksamkeit umzusetzen. Insofern ist eine Planungssicherheit im Einzelfall sicherlich herstellbar, wenn auch mitunter mit kürzeren Fristen für die technischen Klarstellungen im Rahmen der delegierten und implementierenden Rechtsakte.

„Eine Lösung der Problematik des Zugriffs von demokratisch legitimierten Sicherheitsbehörden auf Daten in der Cloud ist nur politisch herbeizuführen."

BvD: Das Trendthema in den letzten Monaten ist Cloud-Computing. Die EU-Kommission überlegt sich aktuell auch Musterformulierungen dazu. Welche Änderungen werden durch die EU-DSGVO-E zu einer rechtssichereren Grundlage führen?
Albrecht: Eine Verarbeitung in unsicheren Drittstaaten ist nun nach Art. 42 EU-DSGVO-E auch möglich, wenn keine Standardvertragsklauseln verwendet werden, sofern die Kernregelungen aus den in Art 42 Abs. 1a EU-DSGVO-E zitierten Regelungen mit dem Datenimporteur vereinbart werden. Gemäß den Vorgaben der EU-DSGVO-E können dann auch Auftragsverarbeiter als Datenexporteur auftreten, sofern sie vertragliche Regelungen mit den Inhalten der Standardvertragsklauseln oder den Kernregelungen aus Art. 42 Abs. 1a EU-DSGVO-E mit dem Datenimporteur abschließen. In

etlichen Konstellationen bringt dies eine Erleichterung für die beteiligten Unternehmen.

BvD: Warum wird bei der Auftragsverarbeitung die – bisher nach BDSG – eindeutige Verantwortlichkeit beim Auftraggeber aufgegeben und dem Auftragsverarbeiter eine eigene Verantwortlichkeit zugesprochen?
Albrecht: Auch nach dem EU-DSGVO-E bleibt der für die Verarbeitung Verantwortliche immer der allein Verantwortliche. Den Auftragsverarbeiter sollen aber in den Fällen bestimmte Pflichten auferlegt werden, die sich nicht aus dem Auftrag ableiten, sondern den Auftragnehmer originär treffen. Dies betrifft in der Praxis hauptsächlich das Massengeschäft, das sich an eine große Anzahl von Kunden richtet, die in dieser Konstellation aber wenig Möglichkeiten der Einflussnahme hinsichtlich technischer und organisatorischer Schutzmaßnahmen haben.
Hier muss der Auftraggeber darauf vertrauen können, dass unabhängig von den vertraglichen Vorgaben der Auftragnehmer einen Mindeststandard im Interesse der verarbeiteten Daten einhält.

BvD: Bei der Auftragsdatenverarbeitung muss sich weiterhin der Auftraggeber ein Bild von der Datenschutzkonformität machen. Warum kann sich der Auftraggeber von dieser Verpflichtung nicht entlasten, wenn der Auftragsdatenverarbeiter über ein entsprechendes Zertifikat bzw. eine Selbstverpflichtung deren Einhaltung testiert wird? Wird dadurch nicht der Rechenzentrumstourismus gefördert?
Albrecht: Die Abwehr von Kontrollen vor Ort durch eine Zertifizierung oder ein Siegel sehe ich derzeit nicht umsetzbar, da es europaweit an geeigneten Zertifikaten fehlt, die dafür in Frage kämen. Zu deren Entwicklung geben wir nun Anreize. Die EU-DSGVO-E sieht aber auch keine Pflicht zur Kontrolle vor Ort vor. Dies ist keine Forderung aus der EU-DSGVO-E. Die Überprüfung kann auch anderweitig erfolgen.

BvD: Viele Cloudmodelle leben von der internationalen Ausrichtung. Wie geht die EU-DSGVO-E damit um, dass in zahlreichen demokratischen Ländern den Sicherheitsbehörden ein – in der Regel gesetzlich legimitierter - Zugriff auf die Daten eingeräumt wird?
Albrecht: Bei diesem Thema kommt die EU-DSGVO-E an ihre Grenzen. Der Aufhänger für diese Frage in der EU-DSGVO-E ist die Angemessenheit des Schutzniveaus in dem Drittstaat. Wir wollen dem Datenexporteur auch nicht vorschreiben, nur einen Auftragsverarbeiter einzusetzen, der sich nicht „compliant" gegenüber seinen Behörden verhält – zumal, wenn es sich um politisch anerkannt demokratische Rechtsstaaten handelt. Eine Lösung ist nur politisch herbeizuführen, z.B. durch bilaterale Vereinbarungen zwischen der EU und dem Drittland. Um auf der sicheren Seite zu sein, sollten m.E. nach Daten im EU-Inland verarbeitet werden, um den Zugriff ausländischer Sicherheitsbehörden auszuschließen.

„Ein Abschluss des Gesetzgebungsverfahrens wird noch vor der Europawahl 2014 angestrebt."

BvD: Wie geht das Gesetzgebungsverfahren nun weiter?
Albrecht: Bis zum 27. Februar 2013 haben die anderen Fraktionen nun Gelegenheit, Änderungsanträge einzureichen. Die beratenden Ausschüsse können bis März ihre Stellungnahmen abgeben.
Die Orientierungsabstimmung im federführenden Ausschuss, dessen Berichterstatter ich bin, findet Ende April statt. (Anmerkung der Red.:zwischenzeitlich verschoben auf Ende Mai) Je nach Verhandlungsstand im Rat können die Verhandlungen zwischen Parlament, Rat und Kommission (Trilogverfahren) ab Mai 2013 beginnen. Parlament und Rat müssen dem Ergebnis dann mit Mitentscheidungsverfahren zustimmen. Alle Beteiligten wollen dies noch vor der Europawahl 2014 ermöglichen."

BvD: Was hat Sie während des bisherigen Verfahrens am meisten überrascht?
Albrecht: Ich bin immer noch verwundert, dass in einigen Teilen der Wirtschaft Datenschutz und die Grundrechte der Bürger als Einschränkung empfunden werden. Hier fehlt die Weitsicht, dass nur Verfahren und Dienstleistungen, die das Vertrauen der Bürger und Kunden finden, auch nachhaltig Erfolg haben werden. Bereits heute merken wir, wie das Vertrauen in der Bevölkerung rasant abnimmt und die Potenziale datenschutzfreundlicher Angebote immer größer werden. Hier sollte die Europäische Union Vorreiterin werden.

Herausragende Sprecher bei den Datenschutztagen

Zur großen BvD-Veranstaltung haben sich unter anderem die Justizministerin und der Bundesdatenschutzbeauftragte angekündigt

Mit dem Thema „Datenschutz – Gestalten statt Verwalten“ setzen sich die BvD-Datenschutztage 2013 in Berlin auseinander. Am 24. und 25. April werden verschiedene Fachleute in Vorträgen ihre Sichtweise von einem gestaltenden Datenschutz vorstellen. Zum Thema Datenschutzgesetzgebung in der EU werden sich unter anderem Bundesjustizministerin Sabine Leutheusser-Schnarrenberger und EU-Parlamentarier Jan Philipp Albrecht äußern. In Workshops werden die Ideen und Konzepte mit Beispielen aus der Praxis verknäpft. Parallel bietet der BvD drei Praxisseminare an.

„Wer das komplexe Thema Datenschutz nicht nur verwalten sondern aktiv gestalten möchte, von dem werden neben Kompetenz und Sachverstand auch ein Gespür für die Prozesse und die daran beteiligten Personen verlangt“, erklärt BvD-Vorstandsvorsitzender Thomas Spaeing. „Die BvD-Datenschutztage haben sich zu einem festen Termin für Datenschutzbeauftragte entwickelt, die

Termin

BvD-Datenschutztage 2013
24. und 25. April 2013
NH-Berlin Mitte
Infos und Anmeldung unter
https:/www.bvdnet.de

Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, wird die Keynote halten.

Seminare

Am ersten Tag (24. April) der BvD-Datenschutztage bietet der BvD drei Seminare an. Alle Infos dazu finden Sie im Terminkalender auf Seite 69 und im Internet unter https://www.bvdnet.de

sich auf den aktuellen Stand der Diskussionen zum Thema Datenschutz und zu den aktuellen Entwicklungen, insbesondere auf europäischer Ebene, bringen möchten."

Aus diesem Grund freut sich der BvD besonders, dass mit Sabine Leutheusser-Schnarrenberger die Bundesjustizministerin ihr Kommen zugesagt hat. Sie wird am Donnerstag, 25. April, über die Entwicklung des Datenschutzes sprechen. Live aus Brüssel zugeschaltet sein wird Jan Philipp Albrecht, Mitglied des Europäischen Parlaments und dort Berichterstatter zum Datenschutz (siehe auf das Interview ab Seite 12 in diesem Heft). Er wird zum aktuellen Stand der EU-DSGVO-E Auskunft geben.

Bundesjustizministerin Sabine Leutheusser-Schnarrenberger ist Rednerin auf den BvD-Datenschutztagen 2013 in Berlin. (Foto: Bundesjustizministerium)

Über weitere Herausforderungen im Beschäftigtendatenschutz wird Michael Frieser, Integrationsbeauftragter der CDU/CSU-Bundestagsfraktion, Mitglied im Rechtsausschuss, im Innenausschuss sowie im Ausschuss für Menschenrechte und humanitäre Hilfe, sprechen. Chris Newiger, Konzerndatenschutzbeauftragte der Deutschen Bahn AG, wird schließlich über die Bedeutung des Datenschutz in einem Großkonzern wie der Deutschen Bahn sprechen. Die Keynote wird Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, halten.

Nach dem Mittag stehen insgesamt 16 verschiedene Workshops in drei Blöcken auf dem Programm. „Den Teilnehmern steht so eine breite Auswahl an relevanten Praxis-Workshops zur Verfügung, die wichtige Punkte aus den Vorträgen vom Vormittag vertiefen werden", erklärt der stellvertretende BvD-Vorsitzende Jürgen Hartz. Parallel findet im Veranstaltungshotel NH-Berlin Mitte wieder eine Ausstellung mit Partnern des BvD statt. „Auch hier konnte der BvD das Angebot noch ausweiten", sagt Jürgen Hartz.

„In den letzten Jahren haben sowohl die BvD-Mitglieder als auch die Referenten und Gäste des BvD die Veranstaltung gelobt und Anregungen gegeben, die wir aufgenommen und umgesetzt haben", sagt Thomas Spaeing. „Wir freuen uns, dass wir wieder ein umfangreiches Programm aus hervorragenden Keynotes, intensiven Workshops und fundierten Seminaren auf die Beine stellen konnten, um das Thema Datenschutz auf nationaler wie europäischer Ebene zu beleuchten." Der Vorstandsvorsitzende setzt auf einen breiten Austausch zwischen den teilnehmenden Datenschützern. „Erfahrene Datenschützer geben uns aktuelle Denkanstöße und analysieren die kommenden Aufgaben der Informationsgesellschaft. Besonders willkommen ist vielen Teilnehmern daher sicherlich der lockere fachliche Austausch mit den anwesenden Experten, und auch der soll dieses Jahr wieder ausreichend Raum erhalten.

Ihr kompetenter Berater rund um den Datenschutz: Datenschutz-Kompendium, Band II

Exklusives Angebot für BvD-Mitglieder: Jetzt nutzen über beiligenden Flyer

Nutzen Sie das Datenschutz-Kompendium Band II als Nachschlagewerk für Ihre tägliche Datenschutzarbeit!

Neue Kommunikationswege – neue Herausforderungen. Lesen Sie im Band II alles rund um die Themen E-Mail, Internet und Co. und worauf Sie als Datenschutzbeauftragter beim Einsatz neuer Kommunikationswege achten müssen. Nutzen Sie die praktischen Muster und Checklisten für Ihre Datenschutzarbeit mit der beiliegenden CD-ROM.

Ihre Vorteile:

- Leicht verständliche Tipps und Tricks für den Umgang mit neuen Medien
- Beraten Sie Ihr Unternehmen weiterhin kompetent und fundiert – auch bei neuen Themen
- Profitieren Sie von Expertenwissen
- Erleichtern Sie sich Ihre Datenschutzarbeit und nutzen Sie die zahlreichen Muster und Checklisten mit der beiliegenden praktischen CD-ROM
- Verschaffen Sie sich einen Überblick über die neuen Regelungsvorhaben im Datenschutz

So unterstützt Sie dieses Kompendium bei Ihrer Tätigkeit

Als Datenschutzbeauftragter werden Sie täglich Herausforderungen zu meistern haben. Denken Sie etwa an die Prüfung von Verarbeitungsverfahren oder die effektive Schulung von Mitarbeitern. Gerade wenn Sie noch nicht allzu lange den Job des Datenschutzbeauftragten machen, stellt sich schnell die Frage: „Wie gehe ich nur am besten vor?“

Genau hier setzt dieses Buch an. All diejenigen Themen, die die Arbeit des Datenschutzbeauftragten bestimmen, sind praxisnah erläutert: Sie erhalten zahlreiche Tipps, Checklisten und Muster, damit Sie die Theorie schneller und effektiver in die Praxis umsetzen können. Schließlich müssen Sie Ihr Unternehmen, dessen Leitung und Beschäftigte, für den Datenschutz sensibilisieren und zu sich ins Boot holen. Nur so schaffen Sie es, dass das Thema Datenschutz in Ihrem Unternehmen zum Selbstläufer und damit auch zum Erfolgsmodell wird.

Als BvD-Mitglied erhalten Sie das Datenschutz-Kompendium Band II zum Exklusivpreis von 67,45 Euro. Bestellen Sie jetzt über den beiligenden Flyer.

Der Steuerberater zwischen Funktionsübertragung und Auftragsdatenverarbeitung

Durch bewusste gesetzgeberische Entscheidungen im Rahmen des StBerG agiert ein Steuerberater weisungsunabhängig

In der letzten Zeit haben sich Anfragen und Aufsätze in Fachzeitschriften zur Thematik der Beurteilung der Tätigkeit des Steuerberaters unter datenschutzrechtlichen Gesichtspunkten gehäuft. Dies verwundert, denn bereits 1981 beschäftigten sich die Aufsichtsbehörden mit dem Einsatzes des Steuerberaters im Rahmen der Frage der genauen Definition der „Datenverarbeitung im Auftrag" und legten dabei fest, dass diese nur dann vorläge, „wenn der Hauptzweck des Auftrags auf die Verarbeitung von Daten für einen anderen gerichtet ist. Liegt der Hauptzwecke der Dienstleistungen in der Erfüllung einer über die Verarbeitung personenbezogener Daten hinausgehenden Gesamtaufgabe wie z. B. bei der Durchführung der Steuerberatung, Wirtschaftsprüfung oder Grundstücksverwaltung unterliegt der „Auftragnehmer" nicht dem Vierten (redaktionelle Anmerkung: damals betraf dies die Auftragsdatenverarbeitung), sondern dem Dritten Abschnitt des Bundesdatenschutzgesetzes, weil er die durch den „Auftraggeber" übermittelten Daten nur als Hilfsmittel für die Erfüllung eines weitergehenden Auftragszweckes verarbeitet."[1]

Steuerberatung als Paradebeispiel für die Funktionsübertragung

Dies fand dann auch Eingang in die Kommentarliteratur. Die Steuerberatung wird allgemein als Paradebeispiel für die Funktionsübertragung genannt.[2] Damit werden die Auftragsverhältnisse umfasst, bei denen der Dienstleister eigene Entscheidungsmöglichkeiten hat, nicht weisungsgebunden agiert und dadurch nach Übermittlung der Daten eine weitere verantwortliche Stelle darstellt. So umfassen die Merkmale der Funktionsübertragung[3]

- dass die Dienstleistung über die weisungsabhängige, technische Datenverarbeitung hinausgeht;
- dem Dienstleister Rechte zur Nutzung an den Daten für eigene Zwecke überlassen sind und er ein eigenes Interesse an der Datenverarbeitung hat;
- der Dienstleister eigene Entscheidungsbefugnisse hinsichtlich des „Wie" und der Auswahl der Daten hat. Die übertragene Aufgabe erledigt er selbständig und der „Auftraggeber" kann auf die Verarbeitung nicht ohne Weiteres Einfluss nehmen.

Neubetrachtung durch Reform des § 11 Bundesdatenschutzgesetz (BDSG)

Durch die BDSG-Novelle II 2009 hat sich nichts geändert

Damit war die Frage der Beauftragung eines Steuerberaters für lange Zeit eindeutig geklärt. Diese Rechtssicherheit kam allen Unternehmen zugute, die sich keine eigenen Steuer- oder Personalbuchhaltung leisten, sondern hierfür den Steuerberater ihres Vertrauens beauftragen. In der datenschutzrechtlichen Beurteilung hat sich auch durch die BDSG-Novelle II in 2009 nichts geändert. In deren Folge haben die Datenschutzbeauftragten innerhalb der verantwortlichen Stellen alle externen Dienstleister ausfindig machen lassen, die mit der Verarbeitung personenbezogener Daten beauftragt sind, um ein bußgeldbewehrtes Fehlverhalten der verantwortlichen Stellen bei der Auftragsdatenverarbeitung (vgl. § 43 Abs. 1 Nr. 2b BDSG) zu vermeiden. Dadurch kommen auch die Steuerberater erneut in den Fokus einer datenschutzrechtlichen Betrachtung. Sofern dann standardisiert die üblichen Kriterien für die Funktionsübertragung zur Anwendung kommen, werden die Aufträge an den Steuerberater feingliedrig auseinander genommen, um dann aufgeteilt nach den einzelnen Leistungen zu unterschiedlichen Ergebnissen zu gelangen.

In der Regel werden dabei keine Zweifel geäußert, dass bei der Steuerberatung (im klassischen Sinne) sowie bei der Finanzbuchführung eine Funktionsübertragung vorliegt. Dies findet sich in den

Die Steuerberatung wird allgemein als Paradebeispiel für die Funktionsübertragung genannt.

Erläuterungen des Bayerischen Landesamtes für die Datenschutzaufsicht zum § 11 BDSG[4] sowie in fast allen gängigen Kommentaren[5].

Lohnabrechnung durch Steuerberater

Bei der Lohnabrechnung kommen aber Einige zu einem abweichenden Ergebnis. Auch in Fachkommentaren sind die Darstellungen nicht einheitlich und in Einzelfällen tragen Umformulierungen bei einer Neuauflage zur Verunsicherung bei[6]. Die bloße Behauptung, dass bei der Beauftragung eines Steuerberaters immer Funktionsübertragung vorliegt[7], überzeugt ohne weitere Begründung keinen Datenschutzbeauftragten, der seinen Arbeitgeber / Auftraggeber vor einem Bußgeld bewahren möchte. Die Subsumtion, also die Unterordnung eines Sachverhalts unter Tatbestandsmerkmale der Auftragsdatenverarbeitung bzw. Funktionsübertragung, bringen einen zunächst nicht so richtig weiter: Natürlich legt der Steuerberater keine Gehaltsmaßnahmen oder eine Tarifgruppierung fest, natürlich entscheidet er nicht über die Höhe der gesetzlich festgelegten Freibeträge bei Zuwendungen oder der Reisekostenerstattungen durch den Arbeitgeber oder über einen Vorschuss. Es liegt dennoch bei der Beauftragung der Gehaltsbuchführung durch einen Steuerberater keine Auftragsdatenverarbeitung vor, da nicht alleine die Regelungen des BDSG für eine abschließende Beurteilung herangezogen werden dürfen.

Berücksichtigt werden müssen auch die Entscheidungen, die der Gesetzgeber bei bestimmten Berufsgruppen der freien Berufe wie z.B. im Steuerberatungsgesetz (StBerG) getroffen hat und die – bei konsequenter Umsetzung – eine Auftragsdatenverarbeitung durch einen Steuerberater ausschließen. Der Steuerberater übt keine weisungsgebundene Tätigkeit aus, sofern er sich im Rahmen des StBerG bewegt. Dies folgt aus der gesetzlichen Festlegung, dass der Steuerberater einen freien Beruf ausübt (§ 32 Abs. 2 StBerG), verbunden mit den im StBerG beschriebenen Aufgaben des Steuerberaters.

Zwar wird in § 1 und § 5 StBerG die Lohnabrechnung nicht explizit als Aufgabe („Hilfe in Steuer-

sachen") des Steuerberaters aufgeführt. Aus dem Umkehrschluss des § 6 Nr. 4 StBerG („Ausnahmen vom Verbot der unbefugten Hilfeleistung in Steuersachen") ergibt sich aber, dass diese Leistung zu den Hilfen in Steuersachen zu rechnen ist, da ebenso Anderen als Ausnahmeregelung zu § 5 StBerG erlaubt wird, Lohnabrechnungen durchzuführen. Somit ist auch die Leistung der „Lohnabrechnung" als Teil der Steuerberatung umfasst, selbst wenn die Steuererklärung nicht durch diesen Steuerberater erfolgt. Dies hat das kurios anmutende Ergebnis zur Folge, dass die Beauftragung der Lohnabrechnung durch einen gewerblichen Dienstleister als Auftragsdatenverarbeitung zu werten ist, bei einem Steuerberater allerdings nicht.[8] Betrachtet man dazu, dass der Steuerberater nicht nur einer schuldrechtlichen, sondern einer berufsrechtlichen Verschwiegenheitspflicht (§ 203 StGB, § 57 StBerG) sowie einem eigenen Bußgeldrisiko wegen fehlerhafter Beratung (§ 411 Abgabenordnung) unterliegt, wird diese Besonderheit schon verständlicher. Der Gesetzgeber strebt mit dem Verbot gewerblicher Tätigkeit (vgl. § 57 Abs. 4 Nr.1 StBerG) an, den Beruf der Steuerberatung zu heben und will damit erreichen, dass der Steuerberater mit der erforderlichen Unabhängigkeit und Unvoreingenommenheit den Mandanten sachgerät berät. Nach dem Bundesgerichtshof ist „das Berufsbild des Steuerberaters ausgerichtet auf den Vorrang der persönlichen berufsspezifischen Leistung vor den wirtschaftlichen Aspekten der Tätigkeit. Es soll verhindert werden, dass der Steuerberater dem für eine Gewerbetätigkeit kennzeichnenden Gewinnstreben auch im Rahmen der Steuerberatung Raum gibt und seine Mandanten deshalb nicht mehr mit der erforderlichen Unabhängigkeit und Unvoreingenommenheit, also nicht mehr sachgerecht, berät oder jedenfalls in einen solchen Verdacht gerät."[9]

Verantwortlichkeit des Steuerberaters

Unbeachtlich ist in diesem Zusammenhang, durch wen die Dateneingabe in ein EDV-System des Steuerberaters erfolgt: der Steuerberater ist verantwortlich für die Richtigkeit der im Rahmen der Verarbeitung an weitere Stellen zu meldenden Daten wie Sozialversicherungsbeiträge, ordnungsgemäße Steuerabführungen, etc. Er ist dies auch, wenn die Dateneingabe in die Kanzleisysteme der Mandant selbst übernimmt, beispielsweise um Kosten zu sparen. Die Arbeitserleichterung durch die Eingabe der Daten durch Mitarbeiter des Mandanten befreien den Steuerberater nicht von seiner Verantwortlichkeit im Rahmen der Mandatierung für die Richtigkeit der Angaben. Die Alternative hierzu ist die Lizenzierung der Eingabeprogramme durch den Mandanten beim Lizenzgeber und die eigenverantwortliche Erhebung, Verarbeitung und Übermittlung an behördliche Stellen und Sozialversicherungsträger durch den Mandanten ohne Mitwirkung durch den Steuerberater.

Die Grenze dieser Privilegierung ist dann dort zu ziehen, wo sich der Steuerberater standeswidrig verhält und sich außerhalb der Grenzen seines freien Berufs und somit gewerblich bewegt. Dies läge nach dem Kammergericht Berlin dann vor, wenn der Steuerberater EDV-Programme ohne jegliches weiteres Beratungsangebot an den Mandanten weitergibt[10]. Dies dürfte eine Variante sein, die in der Praxis sehr selten vorkommt.

Konsequenzen bei Funktionsübertragung

Was ist nun bei einer Funktionsübertragung zu beachten? Weder aus dem BDSG noch aus dem StBerG ergeben sich spezielle Vorschriften an den Inhalt oder die Form der Beauftragung eines Steuerberaters. Aus dem BDSG gelten die üblichen Anforderungen an die Zweckbestimmung der Verwendung der Daten (§ 28 Abs. 5 BDSG). Die Zulässigkeit der Erhebung und Verarbeitung der Daten des Mandanten durch den Steuerberater begründet sich im Rahmen der Erforderlichkeit in § 28 Abs. 1 Satz 1 Nr. 2[11], § 28 Nr. 2 BDSG, wonach das Erheben, Speichern, Übermitteln oder die Nutzung für eigene Geschäftszwecke erforderlich ist soweit berechtigte Interessen vorliegen und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen dem entgegenstehen.[12] Eine bußgeldbewehrte Kontrollpflicht des Mandanten hinsichtlich des Vorliegens angemessener technischer und organisatorischer Maßnahmen zum Schutz der Daten hat der Gesetzgeber bei einer Funktionsübertragung nicht vorgesehen. Dies ließe sich auch nicht mit der Unabhängigkeit der freien Berufe vereinbaren, ebenso ist auch davon auszugehen, dass allein schon durch die berufsrechtliche Verschwiegenheit durch den Berufsträger angemessene Sicherheitsmaßnahmen zu treffen sind, um die Kenntnisnahme Unbefugter auszu-

Hinweise im Text

[1] So in Ziffer 4 des Hinweises Nr. 14 des Innenministeriums Baden-Württemberg zum Bundesdatenschutzgesetz für die private Wirtschaft, veröffentlicht im Staatsanzeiger für Baden-Württemberg vom 01.04.1981

[2] vgl. Bergmann, Möhrle, Herb in Kommentar zum BDSG, Stand Januar 2012, § 11 RN 11a

[3] ebenda, RN 10

[4] vgl. Bayerisches Landesamt für die Datenschutzaufsicht: zu § 11 Abs. 1 in „Auftragsdatenverarbeitung nach § 11 BDSG, Gesetzestext und Erläuterungen", Stand August 2011; veröffentlicht unter www.lda.bayern.de

[5] vgl. Bergmann, Möhrle, Herb, Kommentar zum BDSG, 44. Ergänzungslieferung Stand Januar 2012, § 11 RN 11a; Simitis, 7. Auflage 2011, § 11 RN 28

[6] vgl. aber die Kommentierung bei Simitis in der 6. und der 7. Auflage: Walz in der 6. Auflage bezieht eindeutig Stellung, dass auch die Gehaltsabrechnung durch Steuerberater Funktionsübertragung sei (§ 11 RN 21); bei Petri in der 7. Auflage gilt dies „nur" für die Buchführung allgemein (§ 11 RN 28)

[7] Schmidt-Keßeler: „Im Blickpunkt: Datenschutz und Datensicherheit in der Steuerberaterpraxis" dort „3. Spezialfall Auftragsdatenverarbeitung", Betriebs-Berater 2012 Heft 24

[8] vgl. auch Gehre/Koslowski: „Steuerberatungsgesetz", 6. Auflage 2009, C. H. Beck, § 32 RN 9

[9] so Bundesgerichtshof, Urteil vom 12. Mai 2011 – III ZR 107/10 mwN

[10] so KG Berlin, 12.11.2003, Az: 24 U 373/02

[11] so Bayerisches Landesamt für die Datenschutzaufsicht, Tätigkeitsbericht für 2011/2012, Ziffer 5.1

[12] Oettrich, „Keine Auftragsdatenverarbeitung bei Übernahme der Lohn- und Gehaltsabrechnung durch Steuerberater" in DStR 2012, 1771

[13] vgl. Aufzählung von Hilfspersonen / Berufshelfern bei Tipke/Kruse: Abgabenordnung, 130. Ergänzungslieferung, Stand August 2012, § 102 RN 13; Beck´sches Steuerberater Handbuch 2010/2011, M RN 118; S RN 56

[14] vgl. Fußnote 1

Der Steuerberater soll seine Mandanten mit der erforderlichen Unabhängigkeit und Unvoreingenommenheit beraten.

schließen. Setzt der Steuerberater selbst Dienstleister ein, liegt eine Auftragsdatenverarbeitung zwischen dem Steuerberater und dem Dienstleister vor. Für diese sind die Vorschriften des § 11 BDSG anzuwenden. Der Steuerberater ist dann selbst die verantwortliche Stelle, die diesen Dienstleister sorgfältig auszuwählen hat, die vertraglichen Anforderungen berücksichtigen muss und sich über die Einhaltung der technischen und organisatorischen Maßnahmen beim Dienstleister überzeugen muss (§ 11 Abs. 2 BDSG). Er selbst ist dann in der Verantwortung, dies so zu gestalten, dass er dabei seine berufsrechtlichen Verschwiegenheitspflichten nicht verletzt. Er kann beispielsweise einen Dienstleister einschalten, der als berufsmäßig tätiger Erfüllungsgehilfe gilt.[13]

Ausblick

Die Kriterien und Begründungen für die Sonderrolle des Steuerberaters über die gesetzlich geregelte Stellung eines freies Berufes haben in ihren Feinheiten und Differenzierungen leider noch nicht alle datenschutzrelevanten Kreise erreicht. Wünschenswert ist, dass sich 30 Jahre nach den Festlegungen der damaligen Aufsichtsbehörden[14] bei den Datenschutzbeauftragten, den verantwortlichen Stellen und auch bei manchen Aufsichtsbehörden eine einheitliche Betrachtungsweise und somit Rechtssicherheit etabliert. Dadurch wird vermieden, dass durch eine datenschutzrechtliche Fehlinterpretierung einem Steuerberater ein weisungsabhängiges Vertragsmodell auferlegt wird, welches in Widerspruch zu der Ausübung seines freien Berufes steht.

Zusammenfassung

Durch bewusste gesetzgeberische Entscheidungen im Rahmen des StBG agiert ein Steuerberater weisungsunabhängig. Eine Einstufung des Mandatsverhältnisses als Auftragsdatenverarbeitung kommt daher weder bei der Steuerberatung noch bei der Lohnabrechnung durch einen Steuerberater in Betracht. Für den Mandanten bedeutet dies, dass eine schriftliche Vereinbarung nach § 11 Abs. 2 BDSG sowie die Überzeugungspflicht nach § 11 Abs. 2 Satz 4 BDSG über die Einhaltung von technischen und organisatorischen Maßnahmen im Mandatsverhältnis vom Gesetzgeber nach dem BDSG nicht bußgeldbewehrt gefordert wird.

Autor

Rudi Kramer
Rechtsanwalt,
Datenschutzreferent
DATEV eG
BvD-Vorstand

Mitstreiter für Datenschutz-Auskunftsportal gesucht

Innovationsvorhaben erfolgreich beendet

Das Thema Datenschutz hat in den vergangenen Jahren für Verbraucher/innen rapide an Bedeutung gewonnen. Aus diesem Grund hat das Bundesverbraucherministerium (BMELV) von August 2011 bis Oktober 2012 das Innovationsvorhaben „Datenschutz-Auskunftsportal“ gefördert. Ziel des Portals ist es zum einen, den Aufwand der Verbraucher/innen bei der Wahrnehmung ihres Auskunftsrecht nach § 34 BDSG deutlich zu verringern und Informationen zum Auskunftsrecht über eine zentrale Plattform zu verbreiten. Zum anderen soll es Unternehmen erleichtern, Auskunftsersuchen zu beantworten und ihnen eine Möglichkeit geben, sich im Datenschutz zu profilieren.

Das Innovationsvorhaben wurde von den drei Partnern Consist Software Solutions GmbH – einem IT-Spezialisten aus Kiel, dem Institut für Verbraucherpolitik – ConPolicy GmbH aus dem Rheinland und projektbegleitend im Bereich Datenschutz vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) umgesetzt. Der BvD begleitete die Entwicklung des Vorhabens in einem Projektbeirat (siehe auch den Bericht von Jürgen Hartz in der Ausgabe 01/2012 der BvD-News).

Das Forschungsvorhaben kommt zu dem Ergebnis, dass die Umsetzung des Portals möglich ist.

Es muss jedoch vielfältigen und hohen Anforderungen genügen:

- Verbraucher/innen erwarten ein glaubwürdiges Portal, das sie in wenigen Schritten zu den Auskunftsersuchen führt und Informationen zum Auskunftsrecht bietet.
- Unternehmen wünschen sich ein Portal, das ihnen eine Möglichkeit bietet, Reputation im Bereich des Datenschutzes aufzubauen, eine effektive Beantwortung der erstellten Ersuchen ermöglicht und ein „Spamming“ mit Auskunftsersuchen verhindert.
- Aus Sicht des Datenschutzes muss das Portal vorbildlich datenschutzkonform umgesetzt werden und die Verbraucher in vorbildlicher Weise unterstützen.
- Für die Betreiber kommt es darauf an, das Portal zumindest kostendeckend und mit überschaubaren Risiken zu betreiben.

Wesentliche Ergebnisse: Eine Umsetzung des Portals ist möglich

Um diesen Anforderungen zu genügen, sieht das Labormuster die folgenden fünf Säulen vor:

- Das Portal sollte von einer neu zu gründenden GmbH getragen werden.
- Die Glaubwürdigkeit der GmbH sollte durch einen beratenden Beirat erhöht werden.
- Das „Datenschutz-Auskunftsportal“ stellt die zentrale Anlaufstelle für Verbraucher/innen und Unternehmen dar.
- Die GmbH durchläuft mit seinem Portal einen Zertifizierungsprozess beim ULD, um seine vorbildliche Datenschutzpraxis zu dokumentieren.
- Um Unternehmen weitere Profilierungsmöglichkeiten zu bieten, ist eine Vergabe eines Labels „Datenschutz-Auskunft: Transparentes Unternehmen“ angedacht.

Im Rahmen des Forschungsvorhabens wurde auch ein Labormuster des Portals erstellt. Es zeigt, wie Verbraucher/innen in drei Schritten Unternehmen auswählen, ihre persönlichen Daten eingeben und die Schreiben versenden können.

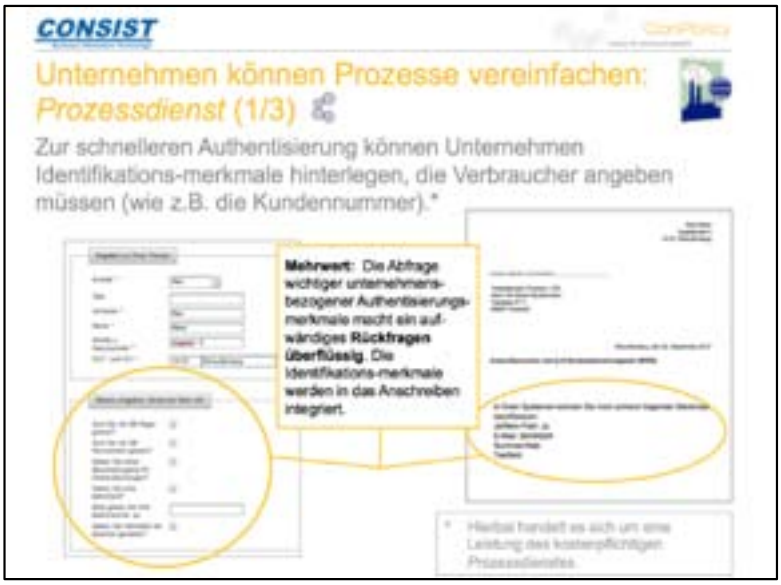
Betroffene können ihre Auskunft nun viel einfacher einholen.

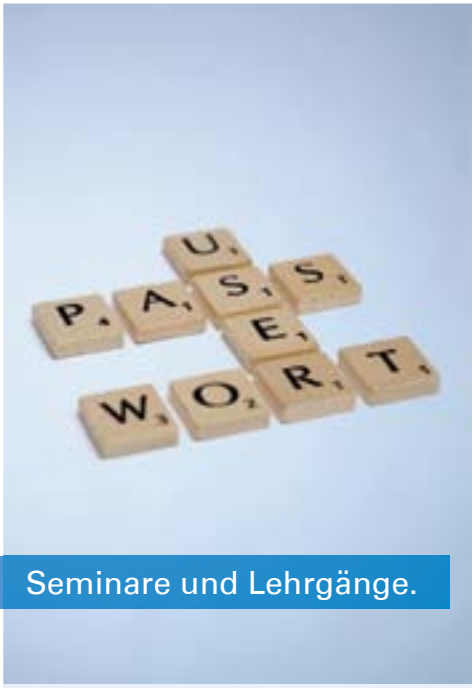
Neben einer einfachen Nutzerführung bietet das Portal Verbraucher/innen auch eine Möglichkeit, sich über ihre Rechte und über die Datenschutzpolitiken von Unternehmen zu informieren und sich mit anderen Nutzern und den Unternehmen über ihre Erfahrungen mit der Beantwortung der Auskunftsersuchen auszutauschen.

Preview des Datenschutzauskunftsportals

Unternehmen können ihre Prozesse durch das Portal stark vereinfachen. So ermöglicht das Portal beispielsweise Unternehmen, die den Prozessdienst gebucht haben, Identifikationsmerkale zu hinterlegen. Kunden werden im Prozess der Auskunftsgenerierung etwa nach ihrer Kundennummer gefragt. Diese wird dann in das Auskunftsersuchen integriert und erleichtert Unternehmen die Authentisierung.

Überdies können Unternehmen im Auskunftsprozess hinterlegen, ob Verbraucher/innen den Schreiben Unterlagen (wie etwa eine geschwärzte Personalausweiskopie) beifügen müssen. Zur zielgerichteten Adressierung können Abteilungen oder Personen hinterlegt werden. Auch wird ein Widget zur Integration in die Unternehmenswebsite zur





Seminare und Lehrgänge.

Für eine gesetzeskonforme und professionelle Umsetzung
Der Bereich Training und Consulting von TÜV Rheinland bietet ein breit gefächertes Portfolio an Bildungs- und Beratungsdienstleistungen auf höchstem fachlichem Niveau. Mehr als 7.500 Angebote, über 2.500 Referenten. Deutschlandweit. Und darüber hinaus.

Auch zum Thema Datenschutz und Compliance bieten wir zahlreiche Seminare und modulare Lehrgänge mit der Möglichkeit, ein Zertifikat der unabhängigen Personenzertifizierungsstelle PersCert von TÜV Rheinland zu erwerben:

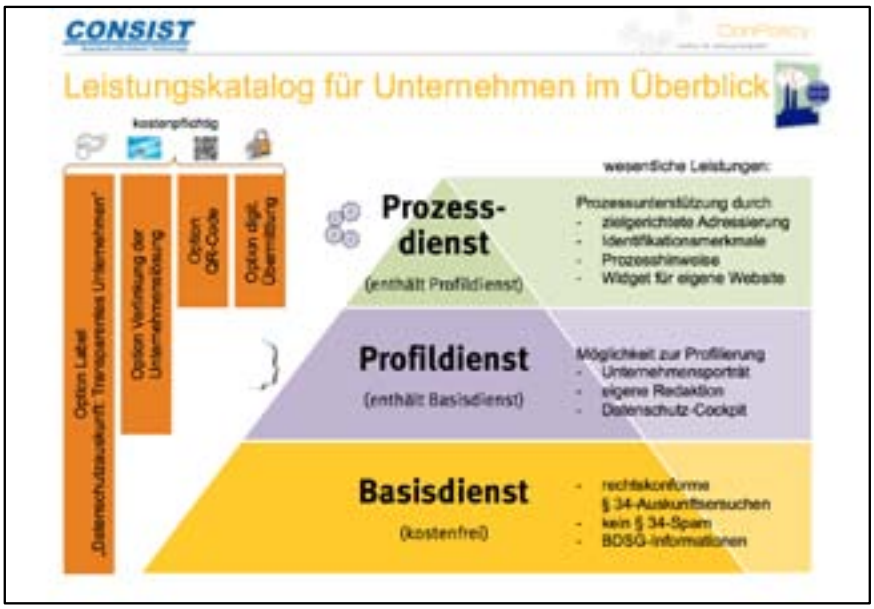
Datenschutz
- Datenschutzassistent
- Datenschutzbeauftragter (TÜV)
- Datenschutzmanager
- Datenschutzauditor (TÜV)
- Externer Datenschutzbeauftragter (TÜV)

Compliance
- Compliance Officer (TÜV)
- Compliance Auditor (TÜV)

Mitglieder des BvD erhalten im Jahr 2013 bei Teilnahme an den genannten und weiteren definierten Seminaren zum Thema Datenschutz und/oder Compliance einen Preisnachlass.

Weitere Informationen erhalten Sie bei:
TÜV Rheinland Akademie GmbH
Am Grauen Stein · 51105 Köln
Sandra Fahling
Tel. 0221 806-3561
sandra.fahling@de.tuv.com
www.tuv.com/datenschutz
www.tuv.com/compliance

TÜVRheinland®
Genau. Richtig.



Verfügung gestellt. Verfügt ein Unternehmen bereits über eine eigenes Angebot, über das Verbraucher/innen ein Auskunftsersuchen stellen können, kann das Datenschutz-Auskunftsportal auf dieses Angebot verlinken. Überdies kann als Option ein QR-Code in die Ausschreiben integriert werden. Hierdurch können postalisch verschickte Anschreiben automatisiert ausgelesen werden. Zudem kann als Option eine digitale Übermittlung der Anfragen vom Portal an die Unternehmen eingerichtet werden. Die Abbildung oben fasst alle Leistungen zusammen.

Vom Labormuster zur Realisierung: Mitstreiter gesucht

Das Forschungsvorhaben hat jedoch auch aufgezeigt, dass eine erfolgreiche Realisierung von drei Erfolgsfaktoren abhängt, die nicht alleine vom Projektteam beeinflussbar sind:

1. Fortgesetzte Unterstützung des Portals durch namhafte Akteure wie das Bundesverbraucherministerium, die Datenschutz- und Verbraucherorganisationen sowie die Branchenverbände.
2. Deckung der Investitionskosten in Höhe von 500 T€, um das Labormuster auszuentwickeln und die Anlaufkosten für Vertrieb und Betrieb zu finanzieren.
3. Gewinnung von ca. 35 Unternehmen, die die Dienstleistungen des Portals im ersten Jahr (d.h. 2013) buchen.

Das Projektteam konnte einige Zwischenerfolge auf dem Weg zur Realisierung verbuchen: So haben alle wesentlichen Verbände und das Verbraucherministerium (BMELV) ihre weitere Unterstützung grundsätzlich zugesagt. Auch konnten wir ein namhaftes deutsches Unternehmen als potentielles Gründungsunternehmen gewinnen. Allerdings hat es klargestellt, dies nicht als einziges Gründungsunternehmen zu tun.

Insgesamt reicht dieser Zuspruch insbesondere von Seiten der Unternehmen noch nicht aus, das Vorhaben auch tatsächlich zu realisieren. Von daher sucht das Projektteam nach weiteren Mitstreitern.

Gerne steht das Team zur Verfügung, um Fragen zum Datenschutzauskunftsportal zu beantworten und das Labormuster vorzuführen. Wenden Sie sich bei Interesse bitte an: Dr. Christian Thorun - info@conpolicy.de oder 02224 / 187 95 93.

25 Jahre Ausbildung von Datenschutzbeauftragten

Großes udis-Jubiläum wurde in Ulm mit einem Kongress begangen – auch der BvD beteiligte sich an der Veranstaltung

Im Oktober 1987 startete in Ulm die erste Ausbildung von betrieblichen und behördlichen Datenschutzbeauftragten. Vorbilder für eine solche Ausbildung gab es nicht, denn es war die erste Ausbildung dieser Art überhaupt. Hintergrund war der große Leidensdruck, dem viele Datenschutzbeauftragte damals ausgesetzt waren. Denn betriebliche Datenschutzbeauftragte waren zu jener Zeit (wie sehr oft ja auch noch heute) in ihren Betrieben Einzelkämpfer und sie litten meist auch unter den unzulänglichen Rahmenbedingungen ihrer Tätigkeit.

Fast zwangsläufig entwickelte sich aus dieser unbefriedigenden Situation heraus ein Kreis von engagierten Datenschützern, die diese Situation verändern wollten. Zu diesem Kreis gehörten zum Beispiel Rüdiger Dierstein, Bernd Beier und Gerhard Kongehl, etwas später kam dann auch Armin Herb hinzu. Dieser Kreis strebte zweierlei an: Zum einen wollte er eine Ausbildung, zumindest jedoch eine Fortbildung zu wirklich qualifizierten Datenschutzbeauftragten ins Leben rufen, zum anderen eine Interessenvertretung und ein Forum für die betrieblichen Datenschutzbeauftragten schaffen. Aus ersterem ist im Herbst 1987 die erste Ausbildung von Datenschutzbeauftragten entstanden, aus letzterem der 1990 in Ulm gegründete Berufsverband der Datenschutzbeauftragten (BvD). Sieben Jahre später entwickelte sich aus diesen Initiativen udis, die Ulmer Akademie für Datenschutz und IT-Sicherheit.

Am 5. Oktober 2012 waren dann genau 25 Jahre vergangen, seit die Ausbildung von geprüften fachkundigen Datenschutzbeauftragten in Ulm gestartet wurde. Dieses Jubiläum wurde im Ulmer Stadthaus mit einem zweitägigen Kongress gefeiert. Von den bisher etwa 1800 Teilnehmerinnen und Teilnehmern an dieser Ausbildung waren alle eingeladen, soweit deren Adressen noch verfügbar waren. Etwa so viele, wie das Stadthaus und seine

Prof. Dr. Gerhard Kongehl ist einer der Gründer des BvD und der udis.

Gastronomie verkraften konnte, sind dieser Einladung dann auch gefolgt.

Es wurde auf dem Kongress aber nicht nur gefeiert, es gab auch Vorträge und Diskussionen, die sich unter der Überschrift „Datenschutz 0.0 – Die EU-Datenschutzverordnung und das Ende der Privatheit“ mit der heutigen Situation des Datenschutzes und den Perspektiven einer wahrscheinlich kommenden EU-einheitlichen Datenschutzgesetzgebung befassten. Die Teilnehmerinnen und Teilnehmer wurden begrüßt von Ivo Gönner, dem Oberbürgermeister der Stadt Ulm, von Dr. Hans-Walter Roth als Vertreter des Ulmer Stadtrats, von Peter Schaar, dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, von Jörg Klingbeil, dem Beauftragten des Landes Baden-Württemberg für den Datenschutz und von Thomas Spaeing, dem Vorsitzenden des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD). Referenten waren unter anderem ebenfalls Peter Schaar, Jan Philipp Albrecht, der Berichterstatter des Europäischen Parlaments zur geplanten EU-Datenschutz Grundverordnung, Dr. Thomas Petri, der bayerische Landesbeauftragte für den Datenschutz und Professor Dr. Alexander Rossnagel, Professor für Öffentliches Recht der Universität Kassel.

Peter Schaar erklärte bei der „Familienfeier des deutschen Datenschutzes“, es sei an der Zeit, mehrheitsfähige Lösungen für die 27 EU Mitgliedstaaten zu formulieren. Die im Januar 2012 von der EU Kommission veröffentlichten ersten Entwürfe würden aber definitiv zu kurz greifen. Die Datenschützer müssten ihre Stimme in Brüssel deutlich erheben, da die Lobbyarbeit der Privatwirtschaft zur Aufweichung des Datenschutzes mit großem Finanzaufwand betrieben werde. Es reiche nicht aus, dass persönliche Daten vertraulich behandelt werden müssten, nicht unbefugt verändert werden könnten und der Betroffene über sie verfügen könne. Mit weiteren Standards der IT-Sicherheit müsse man dafür sorgen, dass für unterschiedliche Zwecke erhobene Daten, etwa wenn der Mitarbeiter eines Unternehmens auch dessen Kunde sei, nicht zusammengeführt werden können. Auch kritisierte er die bisher hier vorgesehenen Regelungen zur Bestellung von betrieblichen und behördlichen Datenschutzbeauftragten (Anmerkung: Diese sind inzwischen in einer Weiterentwicklung des Entwurfs auf Initiative des BvD und von udis verbessert worden!). Peter Schaar führte weiter aus, dass gut ausgebildete Datenschützer genau das Gegenteil von Bürokraten seien und viele Unternehmen in Europa sich längst bewusst seien, dass ein guter Datenschutz ihre Marktposition verbessert.

Auch Jan Philipp Albrecht forderte in seinem Statement, dass die EU-Verordnung nicht zur Abschwächung der hohen deutschen Standards beim Datenschutz führen darf. Wir Europäer müssten zusammen agieren und dafür sorgen, dass die Datenschutzverordnung zu einem Goldstandard wird. Thomas Petri forderte, dass bei der anstehenden Reform die verfassungsrechtlichen Ordnungen der

Die Resonanz auf den Jubiläumskongress war groß.

Mitgliedstaaten respektiert werden müssten und dass klare zentrale Vorgaben sich in einer EU Verordnung auf das Notwendige beschränken müssten. Den EU-Mitgliedsstaaten sollten dagegen soweit wie möglich auch weiterhin eigene Spielräume eingeräumt werden. Statt um eine Machtkonzentration in Brüssel – und die EU-Verordnung würde zu einer solchen Machtkonzentration maßgebend beitragen – gehe es um einen Wettbewerb der Ideen zwischen den einzelnen Mitgliedstaaten. Solche Ideen würden dringend benötigt, um die ja noch völlig offene Zukunft der Informationstechnologie mit Blick auf die Menschen verfassungsfreundlich gestalten zu können.

Alexander Rossnagel kritisierte vor allem die viel zu bürokratischen Kontrollregeln des Verordnungsentwurfs der, wenn er von vom EU-Parlament und vom EU-Ministerrat verabschiedet wird, unmittelbare Gesetzeskraft in allen europäischen Staaten erlangen würde. Er wies in diesem Zusammenhang auf die vielen, viel zu vielen sogenannten "Delegierten Rechtsakte" hin, die im Entwurf der EU-Datenschutzverordnung enthalten sind. Diese Rechtsakte würden der EU-Kommission nicht nur ermöglichen, die ziemlich allgemeinen Vorschriften ohne Mitwirkung der einzelnen Länder zu konkretisieren, sondern auch allein auf dem Verordnungswege eine Weiterentwicklung der Datenschutzregelungen voranzutreiben, ohne dass die Mitgliedsstaaten der EU hier noch wesentliches beitragen oder ändern könnten. Das sei insbesondere deshalb problematisch, weil man davon auszugehen habe, dass diese Datenschutzverordnung für ein Jahrzehnt oder gar länger gültig bleiben und sich die Informationstechnologie in dieser Zeit auf unabsehbare Weise aber vermutlich ebenso rasant wie bisher weiter entwickeln würde. Das aber bedeute auch neue bisher unbekannte Gefahren für das Persönlichkeitsrecht der von der Datenverarbeitung Betroffenen – ohne das die Parlamente der einzelnen Mitgliedsstaaten hier noch nennenswert Einfluss nehmen oder gar gestalterisch tätig werden könnten.

Die Kongressteilnehmer waren von den Referaten so beeindruckt, dass sie an die Adressen von Brüssel und Berlin einstimmig eine „Ulmer Resolution" gerichtet haben, in welcher es vor allem um die künftige Rolle der Datenschutzbeauftragten nach Verabschiedung der EU-Datenschutzverordnung geht (siehe dort).

Thomas Spaeing nahm als BvD-Vorstandsvorsitzender an der abschließenden Diskussionsrunde teil.

Am Abend des ersten Kongresstages fand im Stadthaus-Restaurant für die Teilnehmerinnen und Teilnehmer ein Festbankett statt, welches von dem Trompeter Joo Kraus und dem Kontrabassisten Florian King musikalisch umrahmt wurde. Joo Kraus, auch ein weithin bekanntes „Ulmer Gewächs" und dazu auch noch Echo-Preisträger, verlieh mit seinem Partner Florian King dem Jubiläumsfest eine ganz besondere Note.

Am zweiten Kongresstag fand unter der Moderation von Dr. Martin Hofmann von der Südwestpresse eine kontroverse Podiumsdiskussion statt, in der es um die Zukunft der Datenschützer bis zum Jahre 2020 ging. An dieser Diskussionsrunde waren LfD Jörg Klingbeil, der baden-württembergische Landtagsabgeordnete Alexander Salomon, Jürgen Geuter („tante") von der datenschutzkritischen Spackeria, Thomas Spaeing vom BvD und Gerhard Kongehl von udis beteiligt. Auch Thilo Weichert, der Landesbeauftragte von Schleswig-Holstein wollte sich an der Diskussion beteiligen und versuchte deshalb extra von Kiel aus mit dem Nachtzug nach Ulm zu kommen. Leider fielen ausgerechnet in dieser Nacht witterungsbedingt im Raum Hamburg alle Züge aus, sodass die Reise für ihn schon in Hamburg zu Ende war. Er hätte Ulm jetzt nur noch zum Ende des Kongresses erreichen können. So sah er sich leider genötigt, um mit Ringelnatz zu schließen „weise, auf den letzten Rest der Reise" zu verzichten. Die Teilnehmerinnen und Teilnehmer des Kongresses haben diesen leider vergeblichen Einsatz ganz besonders gewürdigt.

Autor

Prof. Dr. Gerhard Kongehl
Geschäftsführer und wissenschaftlicher Leiter der udis Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH
Marlene-Dietrich-Straße 5, 89231 Neu-Ulm
Tel: 0731 . 9858856-0
E-Mail info@udis.de

Ulmer Resolution zum aktuellen Entwurf der EU-DSGVO

„Seit 25 Jahren werden in Ulm Datenschutzbeauftragte ausgebildet. Die Dozenten der gemeinnützigen Ulmer Akademie für Datenschutz und IT-Sicherheit (udis) haben in dieser Zeit die Datenschutzpraxis in Deutschland maßgeblich mitgestaltet. Die mehr als 100 Teilnehmer der udis Konferenz zum 25jährigen Jubiläum stellen fest:

Aufgrund der Allgegenwärtigkeit von personenbezogener Datenverarbeitung und ihres inzwischen kulturstiftenden Stellenwerts für die moderne Gesellschaft bedarf es einer breiten Sensibilisierung aller Bürger zum Thema Datenschutz zur langfristigen Wahrung ihrer Interessen in einer Kultur, die zunehmend auf Datenverarbeitung gründet.

Deshalb fordern wir, statt einer bedingten Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten eine generelle Pflicht zur Bestellung eines Datenschutzbeauftragten im Betrieb. Diese generelle Pflicht betrifft alle nichtöffentlichen Stellen, sofern sie nicht eine Ausnahme von dieser Pflicht begründen können.

Das Bestell- bzw. Ausnahmekriterium an der Mitarbeiterzahl der datenverarbeitenden Stelle festzumachen, ist in keiner Weise sinnvoll. Stattdessen ist eine Bewertung über die Anzahl der von einer Datenverarbeitung Betroffenen und der Sensibilität der Daten unter Berücksichtigung des Verarbeitungskontextes (zentrale Großdatenbanken oder Einzelverarbeitung) weitaus zielführender.

Wird durch Betrachtung der genannten Faktoren keine Ausnahme von der Bestellpflicht begründet, sollte die Bestellung eines Datenschutzbeauftragten der zuständigen Datenschutz-Aufsichtsbehörde verpflichtend gemeldet werden. Eine solche Meldepflicht der Bestellung würde eine wesentliche Transparenzsteigerung zur momentanen Situation darstellen.

Nach der Bestellung des Datenschutzbeauftragten muss dessen Unabhängigkeit und Weisungsfreiheit, wie auch seine allgemeine Rechtsstellung gesichert sein.

Der Datenschutzbeauftragte vor Ort kann, im Gegensatz zu zentralen Strukturen, die Informationsgesellschaft von heute auf eigenverantwortliche und unbürokratische Weise zu einer Kultur der Informationsgerechtigkeit begleiten und stellt dabei aus unserer Sicht auch die volkswirtschaftlich interessanteste Perspektive dar.“

gez: Die Teilnehmerinnen und Teilnehmer der udis-Konferenz zum 25jähren Jubiläum der Ulmer Datenschutzausbildung

Ulm, am 6. Oktober 2012

Unterzeichneten unter anderem die Ulmer Resolution (v.l.): Peter Schaar (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Prof. Dr. Gerhard Kongehl (udis), Jörg Klingbeil (Landesbeauftragter für den Datenschutz Baden-Württemberg) und BvD-Vorstandsvorsitzender Thomas Spaeing.

Meilenstein für Datenträgervernichtung

Neue DIN-Norm 66399 gibt konkrete Handlungsschritte vor

Ein Blick ins Jahr 1987 führt nicht nur politisch und gesellschaftlich in eine vergangene Epoche. Die damaligen elektronischen Speichermedien wirken im Vergleich zu den heutigen Datenträgern ebenfalls wie Relikte aus einer anderen Welt. Die Vernichtung von Akten und anderen Datenträgern wurde aber noch bis zum vergangenen Jahr vor allem von jener vor einem Vierteljahrhundert eingeführten DIN-Norm 32757-1 maßgeblich bestimmt – und dies nicht nur in Deutschland.

Die DIN-Norm 32757-1 wurde primär als maschinenbezogene Norm entwickelt. Sie diente dazu, einheitliche Maßstäbe für die Hersteller von Schreddern zu setzen. Eine verbindliche Darlegung der gesamten Prozesskette für die Vernichtung von Akten und Datenträgern wurde damals allerdings noch nicht in die Überlegungen einbezogen. Dies machte sich erst die seit August 2009 existierende Europäische Norm (EN) 15713 zur Aufgabe, die auch die technischen und organisatorischen

Schutzmaßnahmen für die Informationsträgervernichtung beinhaltet.

Kritiker der auf einem britischen Standard basierenden EN 15713 monieren den Empfehlungscharakter des Dokuments, das vielfach sehr unverbindlich formuliert ist und nicht den neuesten Stand der Technik enthält. Ebenso unberücksichtigt blieben viele der in Deutschland geltenden gesetzlichen Anforderungen zur Vernichtung von Informationsträgern, wie sie beispielsweise im Bundesdatenschutzgesetz (BDSG) oder Sozialgesetzbuch (SGB) niedergelegt sind. Da die Auflagen für die Größe der Partikel, sprich die Überreste eines Vernichtungsvorgangs, aufgrund einer Durchschnittsberechnung eine unverhältnismäßig große Abweichung der einzelnen Teilchenflächen voneinander gestatten, werden aus Sicht der Experten in der EN 15713 bestehende Sicherheitsinteressen aufgeweicht.

66399: Dritter Part kommt seit dem Jahreswechsel zum Tragen

Angesichts des technischen Fortschritts, der nicht mehr zeitgemäßen und auf die Maschinenspezifikationen abhebenden DIN-Norm 32751-1 sowie der mit Formulierungsschwächen und Lücken aufwartenden Europäischen Norm entstand im Spätsommer 2009 in deutschen Fachkreisen der Wunsch den kompletten Prozess der Informationsträgervernichtung in eine neue Norm zu gießen, die mit konkreten Handlungsanweisungen aufwarten kann sowie auf Prinzipien der Wirtschaftlichkeit und Angemessenheit basieren soll. Auf Initiative der Rhenus Data Office GmbH gingen Bundesbehörden, Datenschutzexperten von Wirtschaftsunternehmen, Maschinenhersteller und andere im Feld der Akten- und Datenträgervernichtung tätigen Firmen vor mehr als drei Jahren in Klausur. Als Ergebnis präsentierten die Mitglieder dieses DIN-Arbeitsausschusses die neue Norm 66399. Deren ersten beiden Teilbereiche traten im Oktober 2012 in Kraft, der dritte Part kommt seit dem Jahreswechsel 2012/13 zum Tragen.

Einen wichtigen Beitrag zur Entstehung der Norm leistete eine Broschüre der Gesellschaft für Datenschutz und Datensicherheit (GDD), die als Ratgeber am Markt, auf dem zum Teil riesige Qualitätsunterschiede herrschten, von Unternehmen oder Behörden sehr gefragt war. Die Herausforderung bei der Gestaltung der Norm war es, die wichtigsten Punkte der aus 100 Fragen bestehenden GDD-Broschüre zu filtern und entsprechend auszuformulieren. Insofern legt die DIN 66399-1 anhand des aktuellen Standes der Technik und mit Rücksicht auf die Lesbarkeit Grundlagen und Begriffe fest, die es bei der Vernichtung von Datenträgern zu beachten gilt.

Zu den klassifizierten Termini gehören dabei zuvorderst die Schutzklassen und die Sicherheitsstufen. Für eine sichere und erfolgreiche Vernichtung von Informationen ist es von kaum zu unterschätzender Bedeutung, nicht zuletzt auch für einen externen Dienstleister, wo und auf welchen Datenträgern dieses Wissen gespeichert wurde, wer Zugriff darauf hat und welche Wertigkeit der Herr der Daten, die sogenannte Anfallstelle, diesen Informationen unter Einbeziehung aller gesetzlichen Regulierungen beimisst.

So definieren die einzelnen Schutzklassen den Schutzbedarf:

- Schutzklasse 1: Normaler Schutzbedarf für interne Daten
- Schutzklasse 2: Hoher Schutz für vertrauliche Daten
- Schutzklasse 3: Sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten

Die Wahl der jeweiligen Schutzklasse bestimmt somit maßgeblich die zu ergreifenden technischen und organisatorischen Maßnahmen bei der Vernichtung. Die Sicherheitsstufen spielen parallel dazu eine Rolle, wenn es um Aufwand geht, der mit einer (unberechtigten) Wiederherstellung von Daten im Zusammenhang steht. Die höchste Sicherheitsstufe 7 bedeutet beispielsweise, dass die Reproduktion nach dem momentanen Stand von Wissenschaft und Technik unmöglich ist. Die Sicherheitsstufe 1 hingegen erlaubt die Wiederherstellung der Daten ohne besondere Hilfsmittel und Fachkenntnisse, erfordert jedoch einen erheblichen Zeitaufwand.

Da sich ein unterschiedlicher Grad der Sicherheitsstufe aufgrund des benötigten Personal- und Hardwareaufwandes auch in den Kosten niederschlägt, muss hier vom Kunden eine Entscheidung zwischen der Angemessenheit der Prozesse bezüglich des Schutzbedarfs der Daten und des finan-

ziellen Aufwandes für dessen Umsetzung getroffen werden. Die in der Vergangenheit aufgetretenen Datenpannen von Behörden und Unternehmen künden nicht selten von einem in dieser Zwickmühle durch den Datenherrn getroffenen Urteil, das mehr den monetären Interessen als der Informationssicherheit und dem Datenschutz folgte.

Regelungen zur Prüfung einer Maschine festgeschrieben

Selbstverständlich nimmt auch die Materialbeschaffenheit, die in der DIN 66399-2 sechs Kategorien umfasst, Einfluss auf den Vernichtungsprozess und dessen vor- beziehungsweise nachgelagerten Handlungsschritte. Es ist eben ein Unterschied, ob 30.000 bis 40.000 DIN-A4-Seiten Papier oder ein mit dem in etwa gleichen Datenfassungsvermögen ausgewiesener USB-Stick in Daumengröße vernichtet werden sollen.

Die neuen digitalen Datenträger sind nach dem aktuellen Stand der Technik im zweiten Teil der DIN 66399 niedergelegt, der als Fortschreibung der alten „Maschinennorm“ DIN 32757-1 gelten kann. Die in den Sicherheitsstufen festgelegten Partikelgrößen für eine effiziente Vernichtung fallen unterschiedlich aus, da sich die Speicherdichte oder aber auch die Größe der Informationsdarstellung auf dem jeweiligen Datenträger voneinander abweichend darstellt. Hinzu kommt in der DIN 66399-2, dass Regelungen zur Prüfung einer Maschine festgeschrieben worden sind. Denn nur ein tatsächlich nach den Angaben der Norm arbeitender Schredder erfüllt auch die Anforderungen, die für eine sichere Vernichtung von Informationen fixiert wurden.

Das Alleinstellungsmerkmal der Norm 66399 findet sich in ihrem dritten Teil: Wenn der Kunde Schutzklassen und Sicherheitsstufen klassifiziert, führt ihn die Norm zu jenen zu beachtenden und durchzuführenden, dabei klar strukturierten Handlungsanweisungen.

VIWIS

Lösungen für Bildung
>e-Learning >Beratung >Blended Learning

Datenschutz und IT-Sicherheit: Tägliche Herausforderung für Unternehmen

Sorgfältiger und rechtlich einwandfreier Umgang mit Kundendaten, Schutz der eigenen Daten vor Missbrauch und Verlust.

Trainingsmaßnahmen:
Als Lernprogramm oder spielerisch als Parcour
Verschiedene Module.

VIWIS in Kürze

- Innovative Technik für e-Learning, Mobile Learning und Game Based Learning
- Standard- und Individualcontent
- Modulare Lernplattform
- kompetente Beratung

Unternehmen erhalten bei dem Full-Service-Bildungsanbieter alles, was sie für die effiziente Aus- und Weiterbildung ihrer Mitarbeiter brauchen: moderne Softwarelösungen, hochwertige Inhalte und kundenorientiertes Consulting.
Das Angebot von VIWIS ist branchenübergreifend – für mittelständische Firmen bietet VIWIS eine eigene, preisgünstige Weiterbildungslösung.

VIWIS GmbH
Thomas-Dehler-Str. 2, 81737 München
Tel.: +49 89 627577-00
E-Mail: info@viwis.de
Web: www.viwis.de

Deutlich wird diese Klassifizierung anhand der folgenden Tabelle:

Schutzklassen	Sicherheitsstufen						
	1	2	3	4	5	6	7
1	X*	X*	X				
2			X	X	X		
3				X	X	X	X

* Sind per Definition nicht für personenbezogene Daten anwendbar.

Um dem bereits beschriebenen Handlungsspielraum zwischen Angemessenheit und Wirtschaftlichkeit Rechnung zu tragen, können die technischen und organisatorischen Maßnahmen variieren. Beispielsweise können, sofern der Fokus auf dem ökonomischen Prinzip steht, Daten der Schutzklasse 2 (hoher Schutzbedarf) in der Sicherheitsstufe 3 (Reproduktion ist nur mit erheblichem Aufwand durch den Einsatz von Personen, Hilfsmitteln und Zeit möglich) vernichtet werden. Wird jedoch aufgrund der Wertigkeit der Information der Angemessenheit höhere Bedeutung eingeräumt, so können Daten der Schutzklasse 2 auch in der Sicherheitsstufe 5 vernichtet werden. In der Definition der Norm hat dann eine Reproduktion nur unter Verwendung gewerbeunüblicher Einrichtungen und Sonderkonstruktionen sowie unter Zuhilfenahme forensischer Methoden Aussicht auf Erfolg.

Eine Beeinflussung der Sicherheitsstufe durch Vermischen und Verpressen erschwert die Reproduktion des zu vernichteten Materials. Innerhalb der DIN 66399 kann durch diesen Vorgang allerdings nur noch einmal die nächsthöhere Sicherheitsstufe erreicht werden – jedoch maximal die vierte. Ab der Sicherheitsstufe 5 und höher sind die Vernichtungsüberreste direkt „am Messer“ zu erzeugen, also keine Beeinflussung mehr erlaubt.

Unabhängig davon, wie sich der Herr der Daten – und dieser wird er auch unter Einbeziehung eines Dienstleisters aus rechtlicher Sicht bis zur Vernichtung stets bleiben – entscheidet, die DIN-SPEC-66399-3 gibt die technischen und organisatorischen Maßnahmen vor, die die Prozesssicherheit garantieren. Von der Anfallstelle bis zur umweltfreundlichen Verwertung sind hier die zu absolvierenden Schritte genannt. Zum Beispiel sollen papierene Dokumente der Schutzklasse 3 nicht (zwischen)gelagert werden, sondern unverzüglich in die Vernichtung gegeben werden, damit niemand außerhalb des festgelegten Personenkreises Einsicht in die Akten erhält. Im Idealfall wird so eine am Markt bereits vorhandene berührungslose Vernichtung initiiert, in der selbst der Dienstleister aufgrund der verschlossenen, sich erst im (mobilen) Schredder selbst öffnenden Sicherheitsbehälter keinen Kontakt zu den Informationen erhält.

Diese und alle anderen Handlungsanweisungen, die in der neuen DIN 66399 beschrieben werden, tragen maßgeblich zu einem Qualitätssprung bei der Akten- und Datenträgervernichtung bei. Egal, ob dies durch die Anfallstelle direkt geschieht oder von einem Dienstleister vor Ort oder extern durchgeführt wird. Die neue Norm gewährleistet somit noch wirkungsvoller den Schutz von Informationen, die neben personenbezogenen Daten auch wichtige Firmeninterna und damit Know-how betreffen können, gegenüber dem Zugriff unberechtigter Dritter. Die im zuständigen DIN-Ausschuss während der Beratungsphase aus vielen Ländern der Welt eingetroffenen Verbesserungsvorschläge belegen, dass auch die neue Norm wieder weltweit Maßstäbe setzen wird.

Als einer der Initiatoren der neuen Bestimmung und im Namen wohl aller Mitglieder des DIN-Ausschusses, möchte ich abschließend dem Wunsch Ausdruck verleihen, dass sich alle am Markt befindlichen Dienstleister gegenüber der Norm verpflichtet fühlen beziehungsweise die Prüfungen und damit verbundene Zertifikate als Grundlage ihrer Arbeit nehmen. Eine wirkungsvollere Checkliste zur Absicherung der eigenen Geschäftsprozesse, zur Einhaltung von Rechtsvorschriften (unter anderem BDSG und SGB) und zur Verhinderung von Datenpannen kann es aus unserer Sicht nicht geben.

Autor

Gerhard Friederici
ist Datenschutzbeauftragter für die Rhenus Office-Gruppe und ist als Leiter für Sicherheit und Qualität verantwortlich. Ferner gehört Gerhard Friederici dem Arbeitskreis „Stand der Technik in der Datenträgervernichtung“ der Gesellschaft für Datenschutz und Datensicherheit e.V. an und ist Mitglied im DIN-Arbeitsausschuss NA 043-01-51 AA „Vernichten von Datenträgern“ – DIN 66399.

Es kommt, es kommt nicht, es kommt… oder vielleicht doch nicht?

Jochen Brandt kommentiert den Zickzack-Kurs der Bundesregierung zum geplanten Arbeitnehmerdatenschutz

Wer sich zuletzt im Datenschutz in Deutschland blamieren wollte, musste bloß versuchen eine Vorhersage über die Verabschiedung der Novelle zum Beschäftigtendatenschutz zu machen. Im Januar überschlugen sich wieder einmal die Ereignisse und eine Meldung jagte die andere. Doch schauen wir erst einmal noch weiter zurück.

Wollte man die Geschichte von Anfang an erzählen könnte man meine Lieblingsfloskel für Seminare zum Datenschutz benutzen: „Bevor ich zum Thema komme lassen Sie mich kurz die Geschichte des Datenschutzes in den letzten 25 Jahren…". Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert seit 1992 ein solches Gesetz. Seit dieser Zeit ist es dem Gesetzgeber nicht gelungen eine Regelung zu schaffen, sieht man von dem Reförmchen aus dem Jahre 2009 ab. Von ihm hat der Gesetzgeber ausdrücklich gesagt: „§ 32 enthält eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen …soll." (Deutscher Bundestag, 16. Wahlperiode Drucksache 16/13657 S. 20)

Doch zurück in diese Legislaturperiode. Die Koalitionsparteien hatten sich auf einen neuen Anlauf zu Arbeitnehmerdatenschutz geeinigt. Im Mai 2010 wurde ein Referentenentwurf verabschiedet. Allerdings sollte es kein eigenes Gesetz mehr werden, sondern nur eine Ergänzung des BDSG, die §§ 32 bis 32l. Im Juni 2010 wurden Verbände, darunter auch der BvD, zum Thema angehört. Im August wurde der Entwurf im Kabinett verabschiedet. Im November 2010 gab der Bundesrat eine konstruktiv-kritische Stellungnahme ab. Im Februar 2011 kam der Entwurf die erste Lesung, im Mai 2011 gab es eine Expertenanhörung. Und dann: Still ruht der See… Im September 2011 kamen Änderungsvorschläge aus den Koalitionsfraktionen an die Öffentlichkeit und schon im September 2012 gab es Gerüchte, das Thema solle wieder auf die Tagesordnung des Innenausschusses… und nichts…

Anfang Januar 2013 wurde überraschend ein ambitionierter Zeitplan veröffentlicht 16.01. Innenausschuss, Ende Januar 2.und 3. Lesung, also Verabschiedung, im Bundestag. Die Kritik am diesem Entwurf wurde wieder laut und kam von allen Seiten. Bemerkenswert ist vielleicht, dass sowohl Gewerkschaften als auch Arbeitgeberverbände kritisierten, dass dieses Gesetz keine Rechtsicherheit bringen wird. (Ich kann es nicht lassen: Diese Kritik hatte der BvD schon im Mai 2010 geäußert.) Außerdem wurde kritisiert, dass jetzt plötzlich alles ganz schnell gehen soll.

Erster Termin des ambitionierten Zeitplans verstreicht ungenutzt

Aber auch der Januar ist längst verstrichen, das Thema wurde nicht im Innenausschuss und auch nicht im Parlament behandelt. So ist also nicht zu erwarten, dass dieses Gesetz, das keinen der Beteiligten zufrieden stellt, noch verabschiedet wird. Das Thema wird uns aber trotzdem nicht verlassen, auch wenn der Datenschutz europaweit geregelt wird. Für den Datenschutz im Beschäftigungsverhältnis gibt es eine Öffnungsklausel. Er soll weiterhin auf nationaler Ebene geregelt werden. Und so wage ich dennoch eine Prognose: Vermutlich wird man in ferner Zukunft in der Nähe von Berlin an einer einsamen Kreuzung folgenden Dialog hören können: „Estragon: Komm, wir gehen! Wladimir: Wir können nicht. Estragon: Warum nicht? Wladimir: Wir warten auf das Arbeitnehmerdatenschutzgesetz" (Frei nach Becketts „Warten auf Godot")

Jochen Brandt über das Hin und Her zum Arbeitnehmerdatenschutz.

Autor

Jochen Brandt
Mitglied im BvD-Arbeitskreis Recht und Praxis, begleitet das Thema Beschäftigtendatenschutz seit vielen Jahren

„Den meisten Menschen ist ihre Privatsphäre wichtig“

FoeBuD heißt jetzt digitalcourage: Im Interview erklärt Rena Tangens, wie es zur Änderung kam und was der Verein in der Zukunft plant

Seit kurzer Zeit heißt der FoeBuD e.V. digitalcourage e.V. Der Verein setzt sich seit einem Vierteljahrhundert für eine lebenswerte Welt im digitalen Zeitalter ein. Wie es zur Umbenennung kam, welche Ziele der Verein hat und wie er die Auswirkungen der EU-DSGVO sowie des geplanten Arbeitnehmerdatenschutzes einschätzt, erklärt Rena Tangens im Interview mit Michael Braun.

BvD: Aus FoeBuD ist digitalcourage geworden - warum die Namensänderung und was möchten Sie mit dem neuen Namen aussagen?

Rena Tangens: Der alte Name war ein Hacker-Scherz aus den 80er Jahren, den heute nur noch Eingeweihte verstehen. Mit dem neuen Namen hat endlich eine breitere Öffentlichkeit eine Chance zu verstehen, was wir tun. In „digitalcourage“ klingt Zivilcourage an – und Zivilcourage heißt, sich nicht nur still über Missstände zu ärgern, sondern einzugreifen, selber etwas zu tun. Das ist wichtig, denn Bürgerrechte gibt es nicht geschenkt.

BvD: Richtet sich mit dem Namen auch Ihre Arbeit neu aus?

Rena Tangens: Nein, der neue Name vollzieht nur die Entwicklung nach, die die Organisation längst genommen hatte. Wir sind schon lange nicht mehr der kleine Computerclub, sondern eine anerkannte Nicht-Regierungs-Organisation, die sich bundesweit und in Europa in die Politik einmischt – für Bürgerrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter.

BvD: Seit Ihrer Gründung vor 25 Jahren hat sich im Datenschutz eine Menge verändert - zum Positiven oder eher zum Negativen?

Rena Tangens: Sowohl als auch. 1987, als wir uns gegründet haben, war Datenschutz aufgrund der Volkszählungsproteste und der Nähe zu 1984 noch sehr präsent. In der Internet-Blase der 90er Jahren wurde das Thema erstmal als irgendwie lästig und unsexy angesehen – neu, bunt und Kohle machen war angesagt. Und das obwohl Datenschutz eben wegen der Vernetzung immer wichtiger wurde – für Bürger, Verbraucherinnen und für unsere Demokratie. Wir haben nach neuen Wegen gesucht, das Thema zu vermitteln – am besten geht das mit konkreten Beispielen. Und die haben wir mit BigBrotherAwards geliefert. Seit 2000 verleihen wir jährlich die „Oscars für Datenkraken“. Damit haben wir viele Probleme zum ersten Mal an die Öffentlichkeit gebracht, z.B. Kundenkarten, Scoring, RFID-Technik. Die Medien haben ausführlich darüber berichtet. Das Bewusstsein für Datenschutz ist seit 2000 in Deutschland deutlich gestiegen. Das kann man in der europäischen Vergleichsstudie ab 1991 klar sehen.

BvD: Existiert in der bürgerlichen Gesellschaft überhaupt ein Bewusstsein für die Belange des Datenschutzes, seien es die damit verbundenen Rechte oder auch die Gefahren?

Rena Tangens: Durchaus. Das Wissen, dass es da etwas zu schützen gibt, sozusagen den „inneren Vorgarten“, das ist da. Und immer häufiger ist da das mulmige Gefühl in der Magengrube, dass inzwischen jede Handlung im Alltag beim Telefonieren, Einkaufen oder Reisen elektronische Spuren hinterlässt und im Hintergrund Dinge passieren, die wir nicht überblicken können. Es ist auch nicht leicht, Ursache und Wirkung zu erkennen, da die negativen Folgen oft erst später eintreten, sie der Handlung nicht mehr zugeordnet werden können, da manchmal nicht wir selbst, sondern andere Personen betroffen sind und schließlich, weil die Firmen, die unsere Daten sammeln, keinen Klartext über deren Verwendung mitteilen. Die Verbraucher sollen alles von sich preisgeben, die Datensammler hüllen sich in Schweigen von wegen Geschäftsgeheimnis. Das ist ein Ungleichgewicht zwischen einem einzelnen Mensch und einer anonymen Struktur wie in Franz Kafkas „Prozess“. Den meisten Menschen ist ihre Privatsphäre wichtig – aber sie wissen gar nicht mehr, wo sie anfangen sollen, sich zu wehren. Niemand hat Lust, ständig auf der Hut zu sein, immer das Kleingedruckte zu lesen und dann doch durch juristische Spitzfindigkeiten über den Tisch gezogen zu werden.

Es gibt ja einige Verhaltensweisen und sinnvolle Tools, mit denen wir uns individuell schützen können, z.B. im Laden vor Ort statt online kaufen, bar bezahlen, Rabattkarten, Preisausschreiben und anderen Lockangeboten widerstehen, Verschlüsselung für Mails nutzen, einen unabhängigen Mailprovider wählen, andere Suchmaschinen zum Recherchieren ausprobieren und im Browser einstellen – da gibt es schöne Tipps bei www.eine-woche-ohne.de –, HTTPS-everywhere, Ghostery und TOR zum Surfen nutzen.
Doch all das reicht nicht. Was wir außerdem brauchen, sind wirksame Gesetze mit unabhängigen Kontrollen und Sanktionen, ein Stopp für das staatliche Datensammeln auf Vorrat, datenschutzfreundliche Standardeinstellungen bei Software und Dienstleistungen und wir brauchen andere Geschäftsmodelle, die nicht auf Pseudo-Gratis gegen Datensammeln beruhen – für all das streiten wir auf einer anderen Ebene. Diese Arbeit geht nur mit der Hilfe von vielen.

BvD: Wie bewerten Sie den aktuellen Prozess zur Ausgestaltung der EU-DSGVO?
Rena Tangens: Eine einheitliche Regelung für Europa sollte keinesfalls unter den Datenschutzstandard, den wir in Deutschland erreicht haben, zurückfallen. Angesichts der Scharen von Lobbyisten, insbesondere von US-amerikanischen Konzernen, die die Parlamentarier und die EU-Kommission im Sinne ihrer Geschäftsinteressen zu beeinflussen suchen, haben Bürgerrechte und Datenschutz in diesem Prozess einen schweren Stand. Wir bemühen uns, durch Argumente zu überzeugen, zum Beispiel bei Datensparsamkeit, Zweckbindung, der Definition der persönlichen Daten und der Datenportabiliät. Wir bräuchten dringend mehr Unterstützung für diese Arbeit, um den Lobbyisten etwas entgegensetzen zu können – Stellungnahmen auszuarbeiten kostet viel Zeit, und Reisen nach Brüssel sind teuer.
BvD: Und wie sehen Sie die aktuelle Lage zum Arbeitnehmerdatenschutz?
Rena Tangens: Den wenig arbeitnehmerfreundlichen Entwurf der aktuellen Regierung haben wir offensichtlich erfolgreich abwehren können. Nun muss in der nächsten Legislaturperiode ein besseres Gesetz ausgehandelt werden, das den Schutz der Schwächeren gewährleistet. Es ist ein Trauerspiel, dass das seit Jahren keine Regierung geschafft hat.
Was wir für besseren Arbeitnehmerdatenschutz tun können wird bei unserem AktivCongress Netzgesellschaft vom 3. bis 5. Mai 2013 in Hattingen auf jeden Fall eines der wichtigen Thema sein.

Rena Tangens

BvD: Zurück zu digitalcourage: Wo sehen Sie in der nächsten Zeit die Schwerpunkte?
Rena Tangens: Ein Schwerpunkt ist die europäische Datenschutzgrundverordnung, denn wenn sich da die Konzern-Lobbyisten durchsetzen, ist vieles, was Datenschützer erreicht haben, Makulatur. Ein anderer Schwerpunkt wird das Thema RFID-Chips in Kleidung. Die Chips sind zumeist im Textilpflege-Etikett verborgen, können über acht Meter Entfernung per Funk ausgelesen werden und überstehen locker dreimal waschen und zweimal chemisch reinigen. Wir wollen den Handel verpflichten, diese „Schnüffelchips" beim Kauf aus der Ware zu entfernen.
Und am 12. April 2013 verleihen wir die nächsten BigBrotherAwards. Die Preisträger verrate ich natürlich nicht vorab – aber mit einigen davon werden wir sicher auch in Zukunft zu tun haben...

BvD: Welche vereinsinternen Veränderungen stehen an? Suchen Sie noch Mitstreiter?
Rena Tangens: Die digitalcourage-Webseite wird zur Zeit komplett neu gebaut. Gerne würden wir ein zusätzliches Büro in Berlin eröffnen – doch um das zu finanzieren, brauchen wir noch deutlich mehr regelmäßige Unterstützer. Digitalcourage erhält keine staatlichen Förderungen und verständlicherweise auch kein Firmensponsoring, sondern finanziert sich durch Fördermitgliedschaften und Spenden.
Wir freuen uns sehr über neue Mitstreiterinnen und Mitstreiter! Programmiererinnen, Hardware-Spezialisten, Juristinnen, Fotografen, Journalistinnen und auch alle anderen, die sich für Bürgerrechte und Datenschutz engagieren wollen, sind willkommen. Es gibt viel zu tun!

Kontakt

digitalcourage e.V.
(vormals FoeBuD)
Marktstr. 18, 33602 Bielefeld
Tel: 0521-1639 1639
mail@digitalcourage.de
www.digitalcourage.de
www.foebud.org
www.bigbrotherawards.de
Spendenkonto: Kto. 2129799
Sparkasse Bielefeld, BLZ 48050161
https://www.digitalcourage.de/spenden

Datenschutz in der Arztpraxis – Thema für Aufsichtsbehörden?

Räumliche Gestaltung, Umgang mit Patientendaten und technisch-organisatorischen Maßnahmen in der Praxis im Blick

Datenschutzkontrollen in der Arztpraxis - wer will die eigentlich? Beschwerden oder Eingaben von Patienten wegen behaupteter Datenschutzverstöße in Arztpraxen aus dem letzten Jahr lassen sich fast an einer Hand abzählen. Schön wäre es, wenn dies ein Indiz dafür wäre, dass die Datenschutzvorschriften in den Arztpraxen so gut eingehalten werden, dass in der Tat kein Anlass zu Beschwerden bestünde. Bei einer kritischen Reflexion der eigenen Erfahrungen oder bei Gesprächen im Familien- und Freundeskreis über diese Situation lässt sich häufig sehr schnell feststellen, dass eine so zufriedenstellende Situation leider nicht gegeben ist. Für den einen Patienten mag es als völlig normal erscheinen, wenn er am Empfang ausführlich darlegen soll, welche gesundheitlichen Beschwerden ihn in die Praxis geführt haben, während um ihn herum andere Patienten mit aufmerksamen Zuhören ihre Wartezeit überbrücken, oder wenn man mit „Herr Meyer, bitte ins Behandlungszimmer 5 zur Chemotherapie kommen“ aufgerufen wird, und wenn man in dieses Zimmer 5 kommt und auf den Arzt wartet, die eigene Wartezeit damit verbringen kann, die Behandlungsdaten des vorherigen Patienten am Bildschirm intensiv zu studieren. Einem anderen Patienten mögen derartige Erfahrungen mindestens unangenehm sein, aber den Schritt, die Datenschutzaufsicht einzuschalten, beschreitet trotzdem fast niemand, um das Arzt-Patienten-Verhältnis nicht zu beeinträchtigen.

Warum wir Datenschutzkontrollen in der Arztpraxis machen

Wir hatten uns als einen Schwerpunkt unserer Tätigkeit für das Jahr 2012 den „Datenschutz in der Arztpraxis“ vorgenommen und werden unsere

Ein Bereich der Prüfung in der Praxis bezieht sich auf die räumliche Gestaltung: Ist z.B. eine ausreichende Trennung zwischen Empfangs-, Warte- und Behandlungsbereichen gegeben?

Prüfungstätigkeit in diesem Bereich auch im Jahr 2013 fortsetzen. Der Grund hierfür liegt, wie oben ausgeführt, nicht darin, dass so viele oder erhebliche Datenschutzverstöße in Arztpraxen bekannt geworden wären. Es bestehen aber wegen der besonderen Sensibilität von Patientendaten und dem notwendigen Schutz des Vertrauensverhältnisses zwischen Arzt und Patient erhöhte Anforderungen an einen sorgsamen Umgang mit diesen sensiblen Daten. Vor dem Hintergrund der strafbewehrten ärztlichen Schweigepflicht gewinnt das Thema Datenschutz und Datensicherheit für Ärzte und ihre Mitarbeiter eine besondere Bedeutung.

Hinzukommen die Entwicklungen der modernen Informations- und Kommunikationstechnik, die eine zunehmende Vernetzung von Arztpraxen, Krankenhäusern, Apotheken sowie anderen medizinischen Dienstleistern und Patienten ermöglichen. Dies kann zu einer besseren medizinischen Versorgung der Patienten beitragen, da den behandelnden Stellen die erforderlichen Informationen zu ihren Patienten zeitnah zur Verfügung stehen und beispielsweise Doppeluntersuchungen eines Patienten vermieden werden können. Neben den Chancen der neuen Informationstechniken sind jedoch auch die mit dem Austausch großer Datenmengen verbundenen erhöhten Risiken für die übertragenen und in den Arztpraxen verarbeiteten Patientendaten z.B. durch unbefugte Zugriffe von außen zu beachten.

Unser Hauptanliegen bei Datenschutzprüfungen ist dabei nicht, Verstöße festzustellen, um Bußgelder verhängen zu können. Ziel ist es vielmehr, die einzelne Praxis gegebenenfalls auf Versäumnisse hinzuweisen und sie zu unterstützen, den Umgang mit personenbezogenen Daten zu verbessern. Die bisherigen Prüfungen wurden deshalb angekündigt, durch Übersendung eines Fragebogens vorbereitet und terminlich mit dem Arzt so abgestimmt, dass eine Störung des Praxisbetriebs so weit wie möglich ausgeschlossen wurde.

Was prüfen Datenschützer in der Arztpraxis?

Die Prüfung lässt sich im Wesentlichen in drei Bereiche teilen, die räumliche Gestaltung, der Umgang mit Patientendaten und die technisch organisatorischen Maßnahmen in der Praxis.

• Bei der räumlichen Gestaltung wird u.a. darauf geschaut, ob es eine ausreichende Trennung zwischen Empfangs-, Warte- und Behandlungsbereichen gibt, ob Behandlungsunterlagen an der Anmeldung oder im Behandlungsraum vor unbefugten Zugriffen geschützt werden, ob z.B. eine Patientenakte des Vorpatienten noch einsehbar ist, ob Bildschirmschoner verwandt werden, wie ein Bildschirm ausgerichtet und ob bei Telefonaten die Vertraulichkeit gewahrt wird.

• Beim Umgang mit Patientendaten liegt das Hauptaugenmerk darauf, in welcher Art und Weise und an wen Patientendaten weitergegeben werden. Wir prüfen insoweit die Einschaltung von IT-Dienstleistungs-, aber auch Entsorgungsunternehmen für Patientenakten oder elektronische Datenträger, sowie die Weitergabe von Patientendaten an Labore, Unternehmens-, Steuer- und Rechtsberatung sowie privatärztliche Verrechnungsstellen. Ein Kriterium dieses Prüfungsschritts ist u.a. die Frage, ob die notwendigen Verträge vorhanden sind und ob die Überwachungs- und Kontrollpflichten tatsächlich eingehalten werden.

• Bei der Prüfung der technisch-organisatorischen Maßnahmen werden – angepasst an die jeweilige Praxis – Fragen aus einer z.Zt. 15-seitigen Checkliste abgearbeitet, die u.a. von der Art der Schließanlage der Praxis über Passwortnutzung, Regelung der Zugriffsrechte, Einsatz von Virenscannern und Firewall, Regelung des Internetzugangs, Datensicherung, Verschlüsselung, Aufbewahrung der alten Patientenakten bis zur Wartung der Anlagen gehen.

Was haben wir bei den Prüfungen in Arztpraxen festgestellt?

Bei den Prüfungen in den Praxen haben wir insbesondere festgestellt, dass die Gestaltung des Empfangs- und Wartebereichs häufig nicht so ist, dass eine vertrauliche Kommunikation mit den Patienten stattfinden kann. Bei der Einschaltung von Dienstleistern wird nicht immer darauf geachtet, diesen nur die Daten zur Verfügung zu stellen, die unbedingt erforderlich sind. Auch bei der Datensicherung und der Entsorgung gibt es noch Luft nach oben. Dennoch haben die Prüfungen gezeigt, dass den Ärzten und Praxismitarbeitern der Datenschutz ein wirkliches Anliegen ist. Ausdruck dafür ist für uns, dass wir keine derart gravierenden Mängel festgestellt haben, die die Einleitung eines Bußgeldverfahrens notwendig gemacht hätten.

Was haben wir mit den Ergebnissen der Prüfungen gemacht?

Ziel dieser Datenschutzprüfungen war von Anfang an, uns ein Bild von der „gelebten Praxis“ (im doppelten Sinne des Wortes) zu verschaffen, um dann in Kooperation mit den Ärztlichen Kreis- und Bezirksverbänden in ganz Bayern Informationsveranstaltungen anbieten zu können, bei denen wir über unsere Prüfererfahrungen berichten, um andere Ärzte und Praxismitarbeiter zu motivieren, auch in den von uns nicht geprüften Praxen die eine oder andere datenschutzrechtliche Verbesserung vorzunehmen.

Tipps für Ärzte und Patienten

Nicht zuletzt durch die Strafvorschrift des § 203 StGB, die ein unbefugtes Offenbaren von Geheimnissen durch Ärzte, was schon alleine die Mitteilung, dass ein bestimmter Mensch Patient eines Arztes ist, sein kann, sind die Anforderungen an den sorgsamen Umgang mit Patientendaten von herausragender Bedeutung. Eine Datenpanne in einer Arztpraxis stellt deshalb nicht nur einen datenschutzrechtlichen Verstoß, sondern häufig auch die Erfüllung eines Straftatbestandes dar. Ohne die Hauptaufgabe einer Praxis, dass man sich dort um die Gesundheit der Menschen kümmern möge, zu vernachlässigen, sollte jedoch der Pflege des Persönlichkeitsrechts der Patienten ebenfalls die notwendige Aufmerksamkeit gewidmet werden. Patienten haben die Möglichkeit, Hinweise auf Datenschutzverstöße mit der Bitte um vertrauliche Behandlung an die Datenschutzaufsichtsbehörden zu melden, die im weiteren Verfahren dafür Sorge tragen kann und muss, dass die Identität des Patienten nicht offen gelegt wird. Wegschauen ist auch hier nur die zweitbeste Lösung.

Bei der Prüfung wird auch untersucht, wie mit Patientendaten umgegangen wird.

Autor

Thomas Kranig
Präsident Bayerisches Landesamt
für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach
Tel: 0981 / 53-1302
E-Mail: thomas.kranig@lda.bayern.de
Internet: www.lda.bayern.de

So wird der IT-Grundschutz-Standard implementiert

Wie man die Instrumente des Bundesamtes für Sicherheit in der Informationstechnik richtig und angemessen anwendet

Die These, IT-Grundschutz sei nur etwas für große Unternehmen, ist falsch. Mit einer pragmatischen Vorgehensweise kann jedes Unternehmen IT-Grundschutz umsetzen. Entscheidend ist dabei, das richtige Fingerspitzengefühl zu entwickeln, um die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung gestellten Instrumente richtig und angemessen anzuwenden.

Auf der Webseite des BSI werden sehr viele Informationen zum IT-Grundschutz präsentiert, die es dem Interessierten nicht einfach machen, den Einstieg in die Grundschutz-Thematik zu finden. „Wo fange ich an?“ oder „Muss ich etwa alles durchlesen?“ fragen sich „Einsteiger“ häufig. Es entsteht schnell der Eindruck, dass die Informationen zum IT-Grundschutz zu umfangreich sind und der Arbeitsaufwand zum Verstehen und Anwenden zu viel Zeit beansprucht.

Wie finde ich den Einstieg …

IT-Grundschutz lässt sich für alle Unternehmensgrößen, auch für Kleinstunternehmen, umsetzen. Es kommt dabei auf die richtige Anwendung der IT-Grundschutz-Instrumente an. Dies setzt voraus, dass dem Anwender die Grundschutz-Methode bekannt ist. Deshalb sollte er/sie versuchen, zuerst den IT-Grundschutz zu verstehen. Danach kann er/sie umso schneller und effektiver mit der Implementierung im Unternehmen beginnen.

Ein guter Einstieg sind die vom BSI erstellten IT-Grundschutz-Standards 100-1 bis 100-4 (siehe Abb. 1). Sie erläutern sehr ausführlich, welche Voraussetzungen das Unternehmen erfüllen muss und wie IT-Grundschutz anzuwenden ist:

- Standard 100-1 Managementsystem für Informationssicherheit: Im Standard 100-1 werden die Voraussetzungen für die Umsetzung von IT-Grundschutz beschrieben. Grundlage ist ein organisatorisch eingerichtetes Informationssicherheitsmanagementsystem (ISMS), das die Sicherheitsprozesse steuert. Darüber hinaus soll sich die Geschäftsführung mit IT-Sicherheit identifizieren

Abb. 1: IT-Grundschutz auf der Webseite des BSI

und alle für die Umsetzung von IT-Grundschutz erforderlichen Ressourcen zur Verfügung stellen.

• Standard 100-2 IT-Grundschutzvorgehensweise: Für eine effektive Umsetzung von IT-Grundschutz hat das BSI eine bestimmte Vorgehensweise entwickelt. Der Standard 100-2 beschreibt die einzelnen Schritte – Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basissicherheitscheck, Ergänzende Sicherheitsanalyse – der Grundschutz-Methode. Die Methodik baut auf dem Standard 100-1 auf und gibt dem Anwender einen roten Faden für die Umsetzung von IT-Grundschutz.

• Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz: In diesem Dokument wird die Verfahrensweise einer Risikoanalyse beschrieben. Sie ist immer dann umzusetzen, wenn eigene Bausteine erstellt wurden oder im Rahmen der ergänzenden Sicherheitsanalyse für die Bereiche mit hohem oder sehr hohem Schutzbedarf festgelegt wurde, dass eine weitere Risikobetrachtung durchzuführen ist. Dabei ist zu prüfen, welche Gefährdungen für den Informationsverbund durch Grundschutz-Maßnahmen noch nicht ausreichend oder noch gar nicht reduziert wurden. Für die ermittelten Gefährdungen können zusätzliche Maßnahmen festgelegt werden. Es besteht aber auch die Möglichkeit, Gefährdungen durch die Veränderung der technischen Strukturen im Unternehmen aufzulösen.

• Standard 100-4 Notfallmanagement: In dem Standard 100-4 werden Prozesse für den Umgang mit Feuer- oder Hochwasserrisiken sowie für den Ausfall von Informationstechnik (Notfallrisiken) beschrieben. Ein fehlendes Notfallmanagement kann für Unternehmen fatale Auswirkungen haben. Die Festlegung von Zuständigkeiten, die Erstellung von Alarmierungsplänen und die Beschreibung von Wiederanlaufszenarien sollten deshalb berücksichtigt werden.

Darüber hinaus stellt das BSI auf seiner Webseite dem Anwender Leitfäden für kleine, mittlere und große Unternehmen zur Verfügung, in denen die Implementierung von IT-Grundschutz nach der Grundschutz-Methode praxiskonform beschrieben wird. Außerdem werden für den Einstieg Web-Kurse für „IT-Grundschutz", „Notfallmanagement" und für das „Grundschutz-Tool" (GSTOOL) bereitgestellt.

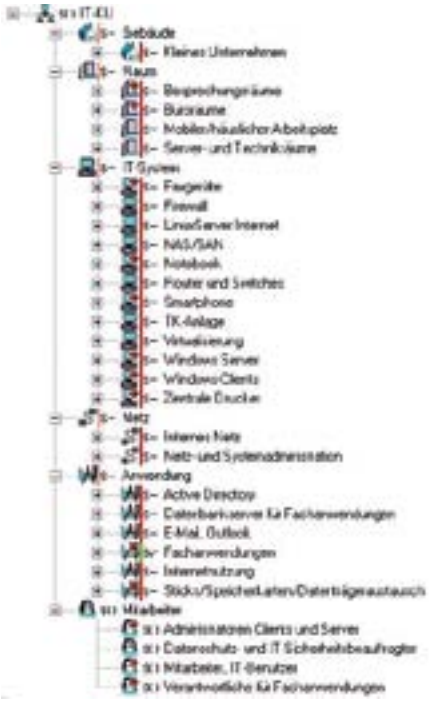


Abb. 2: Kleiner Informationsverbund eines Unternehmens

Bausteine aus den IT-Grundschutz-Katalogen dem Informationsverbund zuordnen …

Für die praktische Anwendung von IT-Grundschutz im Unternehmen hat das BSI die IT-Grundschutz-Kataloge entwickelt. Sie werden jährlich aktualisiert und enthalten derzeit ca. 85 sogenannte Bausteine mit jeweils einem Set von Gefährdungen und Maßnahmen. Jeder Gefährdung steht mindestens eine Maßnahme gegenüber. Die Bedeutung und Anwendung der einzelnen Bausteine wird in den IT-Grundschutz-Katalogen ausführlich beschrieben. Die IT-Grundschutz-Kataloge enthalten also gut strukturiert technische und organisatorische Maßnahmen (Grundschutz-Maßnahmen), die den IT-Grundschutz für das Unternehmen gewährleisten sollen.

Vereinfacht muss das Unternehmen zunächst den Bereich bzw. Informationsverbund in Gestalt von Gebäude, Räume, IT-Systeme, Netze und Anwendungen abgrenzen, für den die Grundschutz-Maßnahmen umgesetzt werden sollen (siehe Abb. 2).

Mit dem Einsatz des vom BSI zur Verfügung gestellten GSTOOL können nach Aufnahme des Informationsverbunds die erforderlichen Bausteine aus den im GSTOOL integrierten IT-Grundschutz-Katalogen ausgewählt und nacheinander bearbeitet werden. Diese Aufgabe erfordert vom IT-Sicherheitsmanagement sehr viel Fachkunde und Fingerspitzengefühl, die IT-Sicherheit in Form von Bausteinen und Maßnahmen für das Unternehmen

Informationsverbund: IT-KU	
Schicht: übergreifende Aspekte	**Schicht: Infrastruktur**
B 1.0 Sicherheitsmanagement B 1.1 Organisation B 1.4 Datensicherungskonzept B 1.5 Datenschutz B 1.6 Schutz vor Schadprogrammen B 1.9 Hard- und Software-Management B 1.11 Outsourcing B 1.13 Sensibilisierung und Schulung zur Informationssicherheit	B 2.1 Gebäude B 2.2 Elektrotechnische Verkabelung B 2.3 Büroraum B 2.4 Serverraum B 2.10 Mobiler Arbeitsplatz B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume B 2.12 IT-Verkabelung
Schicht: IT-Systeme	**Schicht: Netze**
B 3.101 Allgemeiner Server B 3.201 Allgemeiner Client B 3.203 Laptop B 3.301 Sicherheitsgateway (Firewall) B 3.302 Router und Switches B 3.303 Speichersysteme und Speichernetze B 3.304 Virtualisierung B 3.401 TK-Anlage B 3.402 Faxgerät B 3.404 Mobiltelefon B 3.406 Drucker, Kopierer und Multifunktionsgeräte	B 4.1 Heterogene Netze
Schicht: Anwendungen	**Schicht: Risikoanalyse**
B 5.3 Groupware B 5.7 Datenbanken B 5.14 Mobile Datenträger B 5.16 Active Directory B 5.19 Internet-Nutzung bB 5.1 Fachanwendungen	rB 99.5 NAS/SAN rB 99.2 Fachanwendungen

Abb. 3: Bausteinzuordnung für einen kleinen Informationsverbund

angemessen auszugestalten (siehe Abb. 3). Es sollte dabei nicht der Blick in die Praxis verloren gehen. Grundschutz-Maßnahmen sind insbesondere an den Stellen umzusetzen, wo Sicherheitsrisiken festgestellt werden. Dies setzt voraus, dass dem IT-Sicherheitsmanagement die technischen und organisatorischen Strukturen im Unternehmen gut bekannt sind.

Der Umsetzungsstand der Grundschutz-Maßnahmen kann im Rahmen eines Soll-Ist-Abgleichs, dem sogenannten Basissicherheitscheck (BSC), festgestellt und im GSTOOL zu der entsprechenden Maßnahme dokumentiert werden (siehe Abb. 4). Erst nach Abschluss des BSC hat das IT-Sicherheitsmanagement einen Überblick über den Stand der IT-Sicherheit und der Erfüllung des IT-Grundschutz-Standards im Unternehmen.

Sind die Grundschutz-Maßnahmen soweit umgesetzt, ist nach der Grundschutz-Methode für die Bereiche mit hohem oder sehr hohem Schutzbedarf eine ergänzende Sicherheitsanalyse durchzuführen. Es werden also zuerst im Unternehmen die Grundschutz-Maßnahmen der Schutzkategorie „normal“ umgesetzt. Danach soll das IT-Sicherheitsmanagement im Rahmen der ergänzenden Sicherheitsanalyse prüfen, ob trotz umgesetzter Grundschutz-Maßnahmen noch Gefährdungen für die mit der Schutzkategorie hoch oder sehr hoch festgelegten Bereiche vorliegen. Ist dies der Fall, werden die Gefährdungen im Rahmen der Risikoanalyse behandelt und zur Risikoreduktion entsprechende sogenannte zusätzliche Maßnahmen ergriffen. Alternativ wäre auch möglich, die Gefährdungen durch die Umgestaltung des Informationsverbunds aufzulösen.

Zusätzliche bzw. höherwertige Maßnahmen sind bereits in den meisten Bausteinen integriert. Fehlen in den Bausteinen jedoch für die ermittelten Gefährdungen geeignete Maßnahmen, sind vom Anwender eigene Maßnahmen festzulegen und umzusetzen. Die selbst definierten Maßnahmen können dabei entweder vorhandenen oder auch selbst definierten Bausteinen zugeordnet werden (siehe Abb. 5).

Sind auch die im Rahmen der Risikoanalyse festgelegten Verfahrensschritte umgesetzt, ist die

Abb. 4: Ausschnitt Baustein 1.0 – Basissicherheitscheck im GSTOOL

Grundschutz-Implementierung im Unternehmen weit fortgeschritten. Das IT-Sicherheitsmanagement muss nun dafür sorgen, dass der eingeführte IT-Grundschutz-Standard aufrechterhalten bleibt und fortentwickelt wird. Dazu gehört auch die Erstellung und Pflege der Grundschutzdokumentation sowie die Sensibilisierung und Schulung der MitarbeiterInnen für den IT-Grundschutz.

Zusammenfassend in 10 Schritten den IT-Grundschutz-Standard implementieren …

1. IT-Sicherheitsmanagement festlegen: Die Unternehmensleitung legt die Implementierung von IT-Grundschutz in einer IT-Sicherheitsleitlinie fest, benennt die für Informationssicherheit zuständigen MitarbeiterInnen und stattet sie mit den erforderlichen Kompetenzen und Ressourcen aus. Eine Person übernimmt dabei die Rolle des IT-Sicherheitsbeauftragten (ITSB).
2. IT-Grundschutz-Know-how aufbauen: Der/die ITSB informiert sich über die Anwendung von IT-Grundschutz (siehe Abb. 1). Er/sie liest die Standards 100-1 bis 100-4, führt die Web-Kurse durch, macht sich mit der Struktur der IT-Grundschutz-Kataloge vertraut und setzt das GSTOOL ein. Zusätzlich informiert sich der/die ITSB bei Experten über die praxiskonforme Implementierung von IT-Grundschutz.
3. Strukturanalyse durchführen: Der/die ITSB führt eine Bestandsaufnahme der technischen und infrastrukturellen Strukturen im Unternehmen durch. Er/sie nimmt Gebäude, Räume, IT-Systeme, Netze und (Fach-)Anwendungen als Zielobjekte auf und erfasst sie zu einem Informationsverbund im GSTOOL. Bei der Aufnahme der Zielobjekte orientiert er/sie sich an den Bausteinen der IT-Grundschutz-Kataloge (siehe Abb. 2).
4. Schutzbedarf der Zielobjekte festlegen: Der/die ITSB legt in Abstimmung mit der Unternehmensleitung für die Zielobjekte den Schutzbedarf „normal“,

- Externe Datenschutzbeauftragte -
Sie suchen eine Haftpflicht- Versicherung? Sie möchten Ihre bestehende Police vergleichen?
Vermögensschaden-Haftpflichtversicherung - in Zusammenarbeit mit dem BvD entwickelt
Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.
- exclusives Wording für BvD-Mitglieder
- auf Berufsbild und Tätigkeit 'externe DSB' zugeschnitten
- professionelle Beratung mit Betreuung im Schadensfall
jbv Jared Butz
Unabhängiger Versicherungsmakler
Nähere Informationen auch unter www.bvdnet.de (Mitgliederbereich) oder rufen Sie uns an: 06174 - 96843-0
www.jbv-online.de

jbv - Jared Butz unabhängiger Versicherungsmakler Graf-Stolberg-Str. 1-3 61462 Königstein Tel: 06174 - 96843-0 Fax: 06174 - 96843-29 E-Mail: info@jbv-online.de

„hoch“ oder „sehr hoch“ fest. Ziel ist es, dass die Sicherheitsrisiken auf ein akzeptables Maß reduziert werden. Er/sie dokumentiert die Festlegung der Schutzbedarfe mit Begründung im GSTOOL.

5. Bausteine mit Grundschutz-Maßnahmen zuordnen: Der/die ITSB ordnet mit Hilfe des GSTOOLs die Bausteine aus den Grundschutz-Katalogen den ermittelten Zielobjekten zu. Er/sie überprüft, ob für alle Bereiche des Unternehmens Bausteine mit Maßnahmen aus den IT-Grundschutz-Katalogen verfügbar sind. Ggf. definiert er/sie eigene Bausteine mit Maßnahmen oder passt zugeordnete Bausteine aus den Grundschutz-Katalogen an (siehe Abb. 3).

6. Basissicherheitscheck umsetzen: Der/die ITSB überprüft im Rahmen eines Soll-Ist-Abgleichs die zugeordneten Bausteine mit Maßnahmen auf ihre Umsetzung in der Praxis. Dazu befragt er/sie Personen im Unternehmen, die über den Umsetzungsstand Auskunft erteilen können. Ferner dokumentiert er/sie den Umsetzungsstand unter Einsatz des GSTOOLs. Danach ist transparent, welche Grundschutz-Maßnahmen vollständig, nur teilweise oder noch gar nicht im Unternehmen umgesetzt sind (siehe Abb.4).

7. Ergänzende Sicherheits- und Risikoanalyse durchführen: Nach Durchführung des Basissicherheitschecks und nach Umsetzung der meisten Grundschutz-Maßnahmen führt der/die ITSB eine ergänzende Sicherheitsanalyse durch. Er/sie schaut sich im Unternehmen diejenigen Bereiche bzw. Zielobjekte an, für die hoher oder sehr hoher Schutzbedarf festgelegt oder eigene Bausteine angelegt wurden. Dabei überprüft er/sie, ob die umgesetzten Grundschutz-Maßnahmen die Gefährdungen ausreichend reduzieren. Ist dies nicht der Fall, werden im Rahmen der Risikoanalyse für die offenen Gefährdungen ermittelt und zusätzliche Maßnahmen zur Risikoreduktion festgelegt.

8. Schulung und Sensibilisierung planen und ausüben: Der/die ITSB muss die MitarbeiterInnen motivieren und für ausreichende Schulungs- und Sensibilisierungsmaßnahmen sorgen. Sie müssen über Sinn und Zweck sowohl von technischen Sicherheitsmaßnahmen als auch von organisatorischen Vorgaben aufgeklärt werden. Anwender sollten in die Umsetzungsplanung von Maßnahmen mit einbezogen werden. Damit können sie Ideen einbringen und die Praxistauglichkeit von Sicherheitsmaßnahmen beurteilen.

9. IT-Grundschutz-Dokumentation entwickeln und

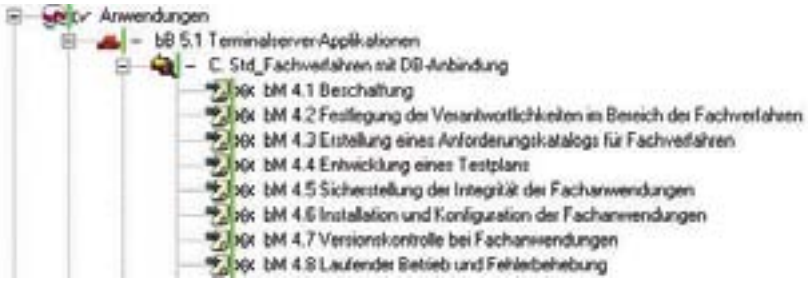


Abb. 5: Ausschnitt benutzerdefinierter Baustein (bB) mit Maßnahmen im GSTOOL

erstellen: Der/die ITSB und MitarbeiterInnen der IT-Abteilung erstellen nach den IT-Grundschutz-Anforderungen Dokumentationsunterlagen. Hierzu gehören z. B. ein Virenschutz- und Datensicherungskonzept, Sicherheitsrichtlinien für Server und Clients sowie Bestandslisten und Netzpläne.

10. IT-Grundschutz intensivieren, aufrechterhalten und kontrollieren: Darüber hinaus veranlasst der/die ITSB die Umsetzung der noch offenen Grundschutz-Maßnahmen. Grundlage ist der mit dem GSTOOL erstellte Basissicherheitscheck. Schritt für Schritt werden die offenen Grundschutz-Maßnahmen im Unternehmen umgesetzt und der aktuelle Stand im GSTOOL dokumentiert. Weiterhin überprüft der/die ITSB im laufenden Betrieb stichprobenartig die Wirksamkeit der umgesetzten Grundschutz-Maßnahmen. Dabei sollen auch technische und organisatorische Veränderungen am Informationsverbund erkannt und notwendige Anpassungen vorgenommen werden.

Hat ein Unternehmen über einen längeren Zeitraum IT-Grundschutz implementiert, kommt häufig auch der Wunsch nach einer offiziellen Bestätigung. Da sich IT-Grundschutz zum internationalen Standard für Informationssicherheit entwickelt hat, bietet das BSI eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz an. Mit einem Grundschutz-Zertifikat ist das Unternehmen in der Lage, die vollständige Umsetzung des Grundschutz-Standards seinen Kunden gegenüber nachzuweisen. Beispielsweise verlangen im Rahmen der Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz Auftraggeber von ihren Dienstleistern zunehmend einen anerkannten Nachweis über die ordnungsgemäße Umsetzung von IT-Sicherheit.

In der nächsten BvD-News: „Welche Anforderungen muss ein Unternehmen für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz erfüllen?“

Autor

Heiko Behrendt
Gutachter und Berater für Datenschutz- und Grundschutzaudits ISO 27001, Grundschutz-Auditor (BSI-ZIG-0167-2012)
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
Tel:0431 / 988-1212
www.datenschutzzentrum.de

Berechtigungen administrieren, dokumentieren und delegieren

Datenschutz und IT-Grundschutz wirksam implementieren

Info

8MAN ist ein Produkt des Berliner Unternehmens protected-networks.com GmbH. Gegründet 2009, entwickelt sie ausschließlich in Berlin und eng mit den Kunden Information Trust Software für das Berechtigungs- und Usermanagement in Windows-Umgebungen von Unternehmen, Behörden und Verbänden. Neben etwa der Deutschen Flugsicherung und der ProSiebenSat.1 Group gehören zahlreiche Kommunen zu den Nutzern von 8MAN.

Geht es darum, sensible Daten zu schützen, hat sich zur Regelung des Alltagsgeschäfts eine komplexe Compliance-Welt aus vertraglichen Regularien und gesetzlichen Vorschriften entwickelt – vom BSI Grundschutz-Katalog über ISO/IEC 2700x, KonTraG, MaRisk etc.

Die Umsetzung dieser Regularien stellt viele Unternehmen vor eine erhebliche Herausforderung. Die oft über Jahre gewachsenen IT-Strukturen sind in der Regel verschachtelt und selbst für versierte Administratoren kaum überschaubar. Steht ein Audit oder eine Umstrukturierung ins Haus, müssen die Berechtigungsstrukturen offengelegt werden. Permanent besteht jedoch das Risiko, dass die undurchsichtige Berechtigungslage zu einem unerkannten Datenleck führt und sensible Daten durch missbräuchlichen internen Zugriff das Unternehmen verlassen.

Eines der zentralen Risiken für internen Datenmissbrauch sind Fehl- und Überberechtigungen. Sie entstehen oft aus ganz alltäglichen Abläufen heraus.

Ein Beispiel: Mitarbeiter Mike Mecker hat während seiner Ausbildungszeit sechs Stationen im Unternehmen Forschgut durchlaufen und ist nach zwei weiteren Jahren Abteilungsleiter. In jeder Abteilung wurden ihm Zugriffsrechte eingeräumt, aber niemand dachte beim Wechsel daran, ihm diese wieder zu entziehen. Das weiß auch Mike Mecker und so gelingt ihm nach seiner Kündigung ein fulminanter Start bei seinem neuen Arbeitgeber – dank der Patentdaten seines alten Unternehmens.

Seinem Nachfolger als Abteilungsleiter, Herbert Unbekannt, werden nach einem kurzen Anruf bei der IT die Rechte seines Vorgängers eingeräumt, schließlich hat er ja dessen Aufgaben übernommen – und damit auch alle Berechtigungen, die sein Kollege in all den Jahren angesammelt hat – ein Alptraum für jeden Datenschützer und doch alles andere als eine Ausnahme.

Geht es um den wirksamen Schutz sensibler Daten vor Missbrauch durch unberechtigte interne Zugriffe, muss sowohl festgestellt werden, wer auf welche Daten warum Zugriff hat als auch sichergestellt werden, dass nicht durch eine unklare Rechteadministration Fehlberechtigungen systemimmanent entstehen. Eine Dokumentation aller Zugriffe und Zugriffsversuche stellt zudem Rechtssicherheit für Administratoren, Abteilungseiter und das Management her – genau diese Punkte sind Basis für eine Zertifizierung nach ISO 2700x bzw. für das Erfüllen der BSI-Standards 100-1 bis 4 sowie des Grundschutzkatalogs.

Wer darf auf welche Daten zugreifen? Wer eine effektive Berechtigungsmanagement-Technologie einsetzt, kann das entsprechend steuern.

Eine sichere, effiziente und transparente Lösung für diese Herausforderungen bietet Information Trust Software, etwa die Technologie 8MAN des Berliner Software Unternehmens protected-networks.com.

Sehen – Administrieren – Dokumentieren – Delegieren

Das können Sie von einer guten Berechtigungsmanagement-Technologie erwarten:

Wer darf wo was warum und wie lange?

• Sehen, wo ein Nutzer berechtigt ist, unabhängig von Gruppenzugehörigkeiten im Active Directory, auf File Servern, SharePoint, Exchange und auf VMware vSphere und das in einer Übersicht
• Erkennen, wer Zugriff auf den Ordner Patentdaten hat, denn alle Berechtigten werden angezeigt und ebenfalls die unterschiedlichen Pfade, durch die sie berechtigt sind
• Wissen, warum derjenige Zugriff hat, wer das genehmigt hat und auf welchem Weg er berechtigt ist

Einfach administrieren und delegieren

• Rechtvergabe und -entzug per drag and drop direkt durch den Fachverantwortlichen dank der anwenderfreundlichen Benutzeroberfläche
• Temporär Berechtigungen vergeben, etwa für externe Berater, Urlaubsvertretungen, Auszubildende
• Rollentrennung zwischen Administrator, Benutzer und Revisor

Dokumentation

• Beweissichere Dokumentation aller Rechteveränderungen in einem bestimmten Zeitraum
• Protokollierung aller Zugriffe und Zugriffsversuche
• Automatische Ausgabe aller Vorgänge für Audits
• Jederzeit kann die komplette Berechtigungssituation dargestellt werden
• Sichert sowohl den Administrator als auch das Management und den Fachabteilungsleiter ab, denn bei Datenmissbrauch kann die Quelle jeglichen unerlaubten Zugriffs aufgedeckt werden

Autor

protected-networks.com

Christian Zander
CPO protected-networks.com GmbH
Alt-Moabit 73
10555 Berlin
www.protected-networks.com

Betrieblicher Datenschutz – erfolgreich umgesetzt

Von den Grundlagen bis zum Datenschutzhandbuch: Eine leicht verständliche Anleitung mit zahlreichen Musterlösungen für den Datenschutzbeauftragten.

» Aktivitäten des Datenschutzbeauftragten
» Anweisungen für die betriebliche Praxis
» Vereinbarungen mit Dienstleistern
» Alle über 30 Textvorlagen, Checklisten, Formulare sind zusätzlich digital in der Mediathek abrufbar: www.beuth-mediathek.de

Bestellen Sie direkt: www.beuth.de/sc/betrieblicher-datenschutz

Beuth Praxis
Betrieblicher Datenschutz
Schritt für Schritt zum erfolgreichen Datenschutzbeauftragten
von Dr. Grit Reimann

1. Auflage 2013. ca. 120 S. A4.
Broschiert.
ca. 58,00 EUR. Erscheint Februar 2013
ISBN 978-3-410-22760-1

Beuth
Berlin · Wien · Zürich

Kontakt: kundenservice@beuth.de | www.beuth.de

Facebook schaltet Gesichtserkennung ab

Erfolg für die Datenschützer in Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat die im vergangenen Jahr gegen die Facebook Inc. erlassene Anordnung aufgehoben. Die Anordnung richtete sich gegen die datenschutzrechtlich unzulässige Ausgestaltung der Gesichtserkennung bei Facebook. Mittlerweile ist diese Funktion europaweit abgeschaltet worden, was das Unternehmen gegenüber dem Hamburgischen Datenschutzbeauftragten plausibel dargelegt hat.

Auch die angekündigte Löschung der bisher erfassten biometrischen Daten ist von der Hamburger Datenschutzaufsichtsbehörde kontrolliert worden. Hierzu hat Facebook überprüfbare Auszüge aus dem benutzten Programmcode vorgelegt. Die dabei gewonnenen Erkenntnisse wurden zudem vom irischen Datenschutzbeauftragten, der eigene Untersuchungen angestellt hat, bestätigt.

In Gesprächen mit Vertretern des Unternehmens wurde darauf hingewiesen, dass umgehend ein neues Verfahren eingeleitet werden würde, wenn die Gesichtserkennung ohne Berücksichtigung der deutschen und europäischen Datenschutzvorgaben erneut eingeführt werden sollte.

„Facebook hat auf unseren Druck reagiert und die rechtswidrige Erhebung personenbezogener Daten eingestellt sowie die zur Dokumentation erforderlichen Auskünfte erteilt. Außerdem wurde zugesagt, dass Facebook zukünftig die datenschutzrechtlichen Vorgaben erfüllen wird. Das Unternehmen weiß, welche unserer Forderungen nicht diskutierbar sind. Hierzu gehört insbesondere eine bewusste und informierte Einwilligung des Nutzers vor jeder biometrischen Erfassung“, erklärt Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.

Medienkompetenz testen

Online-Projekt des Medienkompetenz-Netzwerkes NRW

Das Grimme-Institut hat in Zusammenarbeit mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI NRW) ein Online-Quiz zum Thema „Datenschutz“ vorgestellt. Unter www.mekonet.de/quiz geht es nicht nur um vermeintlich einfache Multiple-Choice-Fragen wie „Was ist ein soziales Netzwerk?“ oder „Welches Passwort ist am sichersten?“.

Jeder Quiz-Teilnehmer bekommt ganz konkret Medienkompetenz vermittelt. Es wird erklärt, an wen man sich bei Datenschutzproblemen wenden kann und welche Folgen es mitunter hat, wenn das Kleingedruckte im Internet nicht gelesen wird. Jede Antwort ist in der Auswertung mit weiterführenden Informationen verknüpft. Zusätzlich zum Thema „Datenschutz“ gibt es vier weitere Quiz-Themen: Internet, Web 2.0, Mobile Media und Computerspiele. Ein zusätzliches Masterquiz wartet mit den schwierigsten Fragen aller Bereiche auf. Für die Nutzerinnen und Nutzer gibt es drei verschiedene Schwierigkeitsstufen. Das Quiz kann online unter www.mekonet.de/quiz abgerufen werden. „Wir betrachten Datenschutz auch als Bildungsaufgabe. Mit dem Quiz kommt ein spielerisches Element hinzu. Das ist eine tolle Sache“, so Ulrich Lepper, Landesbeauftragter für Datenschutz und Informationsfreiheit. Dr. Harald Gapski, mekonet-Projektleiter, freut sich über die Zusammenarbeit mit dem LDI NRW: „Seit Jahren liegt uns das Thema Datenschutz am Herzen, daher freuen wir uns über die Zusammenarbeit mit dem Landesbeauftragten. Unsere Angebote zum Thema Datenschutz – wie etwa die Handreichung „Datenschutz auf einen Blick“ – und auch die bereits vorhandenen Quiz-Themen werden sinnvoll ergänzt.“

Mit ByteAction E-Mails sicher verschlüsseln und archivieren

BAM und BSM 30 Tage kostenlos testen

Wer vertrauliche, digitale Dokumente so sicher und verbindlich wie mit einem postalischen Einschreiben verschicken möchte, kann auf ByteActionMail (BAM) von E-Mail-Management-Experte ByteAction zurückgreifen. Die Vorgehensweise: Der Sender verfasst seine Nachricht als herkömmliche E-Mail, die ByteActionMail verschlüsselt und mit Rückschein überträgt. Nach der Identitätsprüfung erhält der rechtmäßige Empfänger den Nachrichtenschlüssel, um die Datei zu öffnen. Der Absender bekommt im Gegenzug eine E-Mail-Bestätigung über die korrekte Übermittlung der Nachricht. Somit hält BAM die Datenschutzgesetze ein. BAM lässt sich in bestehende E-Mail-Umgebungen wie Microsoft Outlook oder Lotus Notes bzw. in Systeme zur Rechnungslegung oder Lohn- und Gehaltslösungen integrieren.

Vorteile auf einen Blick:
- Einfach ver- und entschlüsseln
- E-Mails an jeden Empfänger der Welt von jedem Endgerät aus
- E-Mail wie ein Einschreiben mit Rückschein - beweisfähig
- Vorhandene E-Mail-Adresse benutzen
- Rechtskonform/Einhaltung des Datenschutzgesetzes möglich

Elektronische Post gesetzeskonform archivieren: Um E-Mails für die lückenlose Nachverfolgung aufzubewahren, eignet sich ein Archivierungssystem wie BytStorMail (BSM). Es speichert automatisch alle ein- und ausgehenden Nachrichten für die gesetzeskonforme Aufbewahrung der Mails nach GdPDU-Richtlinien. Sobald E-Mails eintreffen bzw. versendet werden, erstellt BSM eine Kopie mit Zeitstempel sowie möglicher Anhänge und legt sie im Archiv ab. Virenverseuchte digitale Post und Spam entfernt der integrierte Filter. Über einen personalisierten Web-Zugang lassen sich bei Bedarf Nachrichten wiederherstellen.

Vorteile auf einen Blick:
- Löschen von geschäftsrelevanten E-Mails verhindern
- E-Mails einfach und schnell wiederherstellen
- Beweisfähigkeit bei Rechtsstreitigkeiten
- Für jedes System geeignet – kompatibel zu allen Mailservern
- Keine Änderungen an Hard- und Software

BAM und BSM 30 Tage kostenlos testen: Interessierte können ByteActionMail und BytStorMail 30 Tage kostenlos ohne Risiko oder Verbindlichkeiten testen. Registrierung unter https://sicher.byteaction.de. Infos über die Produkte unter www.byteaction.de.

Info

ByteAction GmbH
Auf der Beune 83-85
64839 Münster
Tel: 06071 / 92160
E-Mail: info@byteaction.de
Internet: www.byteaction.de

ByteAction
GROUP of Internet Companies

Erstmals mehr als 800 Mitglieder im BvD aktiv

Tendenz steigend: Auch im neuen Jahr schon über 40 Anmeldungen

Erstmals verzeichnet der Verband über 800 Mitglieder. Tendenz steigend, denn bis Februar begrüßte der Verband über 40 neue Mitglieder, die sich unserem Berufsverband angeschlossen haben.

Gründe hierfür sind z.B. die starke Vernetzung in den Regionalgruppen und das breite Fortbildungsangebot. Auch das berufliche Leitbild wird immer wichtiger. Für Mitglieder, die extern ihre Dienstleistungen anbieten, ist das ein effektiver Motor zur Kundengewinnung geworden, denn immer mehr Mitglieder berichten, dass im Zuge von Ausschreibungen die Unternehmen Wert auf die Selbstverpflichtung auf das berufliche Leitbild des Datenschutzbeauftragten legen, ebenso auf eine Mitgliedschaft im BvD.

Hier lässt sich deutlich erkennen, dass auch die Übersicht „externe Datenschutzbeauftragte – nach Verbandskriterien verpflichtet“ eine immer größere Rolle spielt, spiegelt sie doch die Qualifikation und auch die Schwerpunktgebiete jedes dort genannten Datenschutzberaters wider.

Der BvD in Zahlen:
802 Mitglieder (Stand Februar 2013)
285 Firmenmitglieder (Stand Februar 2013)
102 registrierte externe Datenschutzbeauftragte (Dezember 2012)
189 freiwillige Selbstverpflichtungen auf das „berufliche Leitbild des Datenschutzbeauftragten“

BvD-Vorstandsvorsitzender Thomas Spaeing freut sich über die positive Entwicklung der Mitgliederzahlen. Über 40 Neumitglieder sind bis Februar hinzugekommen, über 800 sind es mittlerweile insgesamt.

RG Süd wächst weiterhin sehr erfolgreich

Positive Bilanz zum fünften Geburtstag der Gruppe: Über 200 Teilnehmerinnen und Teilnehmer waren seit 2007 dabei

Am 30. Oktober 2007 trafen sich zehn engagierte Datenschützer in den Räumen der Firma ditis in Ulm, um den regionalen Arbeitskreis Süd des BvD ins Leben zu rufen. Die Bilanz nach über fünf Jahren liest sich durchweg positiv: Über 200 Teilnehmerinnen und Teilnehmer waren bislang bei den Treffen des regionalen Arbeitskreises bzw. der Regionalgruppe Süd, wie sie später umgetauft wurde, mit von der Partie

Die große Anzahl der Teilnehmerinnen und Teilnehmer an der ersten Veranstaltung belegte das Interesse an diesem Arbeitskreis. Die Gründungsteilnehmer kamen nicht nur aus dem gesamten Raum Süddeutschlands, sondern garantierten durch ihre unterschiedlichsten Tätigkeiten im Bereich Datenschutz ein breit gefächertes Spektrum an Erfahrungen. Ideale Voraussetzungen um bei den nächsten Veranstaltungen über den eigenen Tellerrand hinauszusehen. Andere Meinungen und Erfahrungen zu den vielfältigen Situationen des Datenschutzes sollen das eigene Wissen bereichern und zu lebhaften Diskussionen anspornen. Die Vielfalt der Branchen aus denen die Mitglieder des neu gegründeten Arbeitskreises Süd kamen, spiegelte sich auch in den Themen wider, die in den zukünftigen Treffen zur Sprache kommen sollen.

Sehr früh machten sich die Teilnehmerinnen und Teilnehmer des Arbeitskreises Gedanken über die Vertraulichkeit der ausgetauschten Informationen innerhalb der Gruppe. Da aber auch Gäste eingeladen werden sollten, musste ein Dokument geschaffen werden, dass dieser Problematik gerecht wurde. Das Ergebnis waren zwei Dokumente, die zum einen das Selbstverständnis der jetzt umbenannten Regionalgruppe Süd des BvD widerspiegelten und eine Vertraulichkeitserklärung, die auch von Gästen unterschrieben werden musste.

Weite Anfahrtswege zu den Treffen nach Ulm und eine immer weiter steigende Anzahl von Teilnehmern führte dazu, dass im Jahr 2010 einige Mitglieder der Regionalgruppe Süd die Regionalgruppe Bayern gründeten. Auch diese erfreut sich an immer weiter ansteigenden Mitgliederzahlen.

Am 7. März 2008 fand das erste reguläre Treffen der Regionalgruppe Süd in Ulm statt. Das Treffen am 22. März 2013 stellt das nach wie vor ungebrochene Interesse an Informationen, Austausch und Diskussionen dar:

- 5 Jahre praxisbezogenen Antworten auf aktuelle Thermen
- 15 Teilnehmerinnen und Teilnehmer im Durchschnitt seit 2010 mit steigender Tendenz
- 16 Treffen ohne Unterbrechung
- 17 Vorträge von internen und externen Referenten
- 200 Teilnehmerinnen und Teilnehmer haben bisher an den Treffen teilgenommen

Diese Zahlen stellen beeindruckend unter Beweis, wie wichtig derartige Plattformen sind. Ob es die neue EU-DSGVO oder andere gesetzliche Änderungen und Vorgaben sind, die vielfältigen und vielschichtigen Aufgaben, mit denen ein Datenschutzbeauftragter tagtäglich zu tun hat, sind kaum zu bewältigen. Die Regionalgruppen des BvD sind Plattform und Netzwerk zugleich. Sie sind unerlässlich um sich auszutauschen, Erfahrungen zu sammeln und andere Meinungen zu hören. Die Neugründungen der letzten Zeit stellen das ungebrochene Interesse an derartigen Netzwerken unter Beweis.

Terminvorschau: Das nächste Treffen der RG Süd findet am 21. Juni 2013 statt. Ein weiterer Termin ist für den 18. Oktober geplant.

Autor

Ulrich Ilgner
Ansprechpartner
RG Süd
E-Mail: rg-sued@bvdnet.de

Mitglieder der RG Bayern diskutieren aktuelle Themen

Beim ersten Treffen standen Sicherheitseinstellungen bei der Microsoft Server 2012-Software im Mittelpunkt

Seit Juni 2010 treffen sich die Mitglieder des BvD e. V. aus Bayern regelmäßig alle 4 Monate unter der Leitung von Stephan Eschenbacher in den Räumen der Microsoft Deutschland GmbH in Unterschleißheim bei München. Die Teilnehmer der Regionalgruppe laden immer wieder Referenten zu unterschiedlichsten Themen ein. So referierte beim letzten Treffen am 8. Februar 2013 Uwe Hoffmann von Microsoft zum Thema „Microsoft Server 2012 Sicherheitseinstellungen“ und gab interessante Einblicke über Anforderungen, Features kombiniert mit wichtigen Hinweisen für den Datenschutzbeauftragten.

Bei einem der letzten Treffen war auch BvD Vorstandsmitglied Stefan Staub anwesend. Er gab interessante Einblicke über die Tätigkeiten des Vorstandes und berichtete aktuell über die Aktivitäten des BvD-Vorstandes in Brüssel. Hauptthema ist dort natürlich die EU-DSGVO. Die Zusammenarbeit mit Politikern gestaltet sich nicht immer einfach und ist sehr zeitaufwändig.

Terminvorschau:
Nächstes Treffen am 28. Juni 2013, geplante Themen IT-Sicherheitsrichtlinie und BYOD, die Referenten kommen diesmal aus den eigenen Reihen. Am 25. Oktober haben wir dann Thomas Kranig, den Leiter des Bayerischen Landesamtes für den Datenschutz, in der Regionalgruppe zu Gast.

BvD-Vorstand Stefan Staub informierte beim RG-Treffen über die Vorstandsaktivitäten, unter anderem zur EU-DSGVO in Brüssel.

Autoren

Regina Mühlich
Stephan Eschenbacher
Ansprechpartner
RG Bayern
E-Mail: rg-bayern@bvdnet.de

AK Externe informiert sich über die DATEV

Erstes Treffen des Jahres fand in Nürnberg statt

Das erste Treffen des AK Externe in 2013 fand in Nürnberg statt. Am ersten Tag folgte man der Einladung des DSB der DATEV, Rudolf Berthold Gerhard, sich vor Ort über die DATEV zu informieren. Als genossenschaftliche Einrichtung der Steuerberater, Rechtsanwälte und Wirtschaftsprüfer ist die DATEV seit ihrer Gründung mit den Thematiken der Datensicherheit und des Datenschutzes beschäftigt.

So zeigte der erste Vortrag am Beispiel einer privaten Cloud, welche Leistungen über und durch DATEV abgewickelt werden, welche Zusammenhänge und Abhängigkeiten dabei bestehen und welche Möglichkeiten zum sicheren Datenaustausch zwischen Unternehmen, Steuerberatern, Behörden, Banken, Finanzämtern, Sozialversicherungsträgern etc. genutzt werden.

Die rechtlichen Hintergründe dieser Leistungserbringung und die Umsetzung der geänderten Anforderungen an die Auftragsdatenverarbeitung durch die BDSG-Novelle 2009 wurden danach erläutert. Dabei wurde auch das Verhältnis zwischen Steuerberater und Mandant erörtert und diskutiert. Inwieweit datenschutzkonforme Leistungserbringung als Marketinginstrument eingesetzt werden kann, erläuterte der Leiter des Fachvertriebs IT. Neben der emotionalen Bindung zu Sicherheit und Verlässlichkeit legte er dar, wie sich in den letzten Jahren die Wertigkeit des Datenschutzes als Auswahlkriterium bei Kunden vergrößerte. Ergänzend hierzu informierte der Vortrag des Oberregierungsrats Manfred Ilgenfritz des Bayerischen Landesamtes für den Datenschutz zum § 42a BDSG. Aktuelle Fälle und die in 2012 im TKG (§ 109a) überarbeitete Meldevoraussetzungen wurden ausgiebig dargestellt.

Wo der Mittelstand seine Sicherheitsvorkehrungen und -maßnahmen überprüfen und einschätzen kann, wurde danach anhand des Online-Fragen-

Die Darstellung des Leistungsportfolios der DATEV als private Cloud (Foto: DATEV)

Die Mitglieder des AK Externe mit ORR Manfred Ilgenfritz und dem DSB der DATEV, Rudolf Berthold Gerhard. (Foto: DATEV)

tools „Sicherheitscheck“ für Unternehmensverantwortliche vorgestellt, welches auf der Seite www.sicher-im-netz.de kostenlos eingesetzt werden kann. Der Ursprung geht auf eine DATEV-Entwicklung zurück, die dann für die Initiative „Deutschland sicher im Netz“ (DSiN) zur Verfügung gestellt wurde und nun allen im Netz kostenlos offen steht. Anhand einfacher Fragen kann eine Selbsteinschätzung zum Sicherheitsniveau festgestellt werden. Über eine „Ampelantwort“ werden dem Nutzer das Ergebnis und mögliche Verbesserungspotenziale deutlich gemacht. Die Nutzung dieses Tools kann auch bei Mandanten zur Sensibilisierung eingesetzt werden. Darüber hinaus gibt es bei „Deutschland sicher im Netz“ Informationsmaterial, das kostenlos downgeloaded und für Sensibilisierungsmaßnahmen eingesetzt werden kann.

Die organisatorischen Maßnahmen zur Sicherstellung der 7x24h Verfügbarkeit des DATEV Rechenzentrums boten Einblick in die Anforderungen und Struktur eines serviceorientierten Unternehmens. Allein durch organisatorische Veränderungen in der Bearbeitung von schwerwiegenden Störungen im RZ-Betrieb konnten die Störungszeiten wesentlich reduziert werden. Der Leiter des IT-Betriebs stellte dar, welche dynamischen Synergieeffekte sich durch die Zusammenziehung der beteiligten Fachleute in einen Raum im Krisenfall ergeben können. Vorteilhaft ist dabei, dass die Mitarbeiter aus den getrennt aufgestellten Rechenzentren in Nürnberg innerhalb kürzester Zeit zusammenkommen können, um gemeinsam die Fehleranalyse und Problembehebung durchzuführen.

Welche Möglichkeiten und Risiken sowie welche rechtlichen Probleme bei dem Trendthema „Bring your own device“ (ByoD) zu beachten sind, wurden aus Sicht der IT-Sicherheit sowie des Datenschutzes dargestellt. Im Ergebnis erscheint allein eine Lösung, bei der private Geräte lediglich als Thin-Client eingesetzt werden dürfen, geeignet, um alle rechtlichen und sicherheitstechnischen Klippen zu umschiffen. Die Durchführung und Herangehensweise sowie die Prüfungstiefe und Prüfungsdauer beim Datenschutzaudit der DATEV wurde anhand von Beispielen dargelegt. Den Abschluss des Tages vervollständigte die Information über die Dienstleistung zur Datenschutzberatung mit Hintergrundzahlen zu Datenschutzanforderungen und Datenschutzbewusstsein in der Steuerberatungskanzlei.

Am zweiten Tag in Nürnberg haben sich die AK-Mitglieder zu einer Tagung getroffen. Der AK-Externe stellt seine Treffen üblicherweise unter einen Themenschwerpunkt. Für Nürnberg war Compliance, Terror- und Korruptionsbekämpfung im Fokus der Tagung. Zu diesem Thema wurde von einem AK Mitglied ein Vortrag (Compliance, Terror-, AEO - Authorized Economic Operators - und Geldwäschegesetz) gehalten. Ein zweiter Vortrag hatte die Zusammenarbeit mit den Aufsichtsbehörden zum Thema. Der AK Externe gibt seinen Mitgliedern auch die Möglichkeit, in einem „Open Space“ Themen zu besprechen, die für die Mitglieder interessant sind. Im „Open Space“ in Nürnberg hat der AK Externe auch die Themen für die weiteren Treffen in diesem Jahr (in Berlin und Salzburg) vorbereitet.

Autoren

Christine Nottrott-Charlton
Jürgen Hartz
Ansprechpartner
AK Externe
E-Mail: ak-externe@bvdnet.de

AK Medizin: Workshop zur Orientierungshilfe KIS

Veranstaltung des BvD-Arbeitskreises bringt Betreiber in den Kliniken, KIS-Hersteller und Datenschutzaufsichtsbehörden zusammen

Die klassische Papierakte als Patientenakte ist in den letzten Jahren aus den Krankenhäusern nahezu verschwunden. Die Patientendokumentation erfolgt im sog. Krankenhausinformationssystem (KIS). Dieses besteht allerdings nicht nur aus einer einzigen Anwendung (Verfahren), sondern aus einer Vielzahl von Anwendungen wie Laborinformationssystem, Röntgendokumentation, Patientenverwaltungssystem, spezielle Befundungssysteme, etc., die alle ihre Daten über Schnittstellen in der „elektronischen Patientenakte", dem Krankenhausinformationssystem zur Verfügung stellen.

Bereits das BDSG (bzw. LDSG und kirchliche Datenschutzgesetze) stellen an die Verarbeitung personenbezogener Daten besonderer Art – wie sie Gesundheitsdaten darstellen – auch besondere Anforderungen. Zusätzlich gelten die teilweise strengeren Anforderungen aus der ärztlichen Schweigepflicht, die im §203 StGB und der ärztlichen Berufsordnung verankert ist.

„Zur Aufgabenerfüllung erforderlich", „Zweckbindung", „Datensparsamkeit", „Einwilligung" erfordern tagtäglich eine Abwägung zwischen schutzbedürftigem Interesse des Patienten und beispielsweise Zugriffsmöglichkeit des Krankenhauspersonals. Ein Berechtigungskonzept, Zugriffsprotokollierung, Löschfristen, Widerspruchsrecht stellen sowohl die

Der AK Medizin – hier ein Foto von einem Treffen am Rande der BvD-Verbandstage 2012 – veranstaltete einen Workshop zur Orientierungshilfe KIS.

Hersteller solcher Systeme als auch die Krankenhäuser als Betreiber der Software vor große Herausforderungen.

KIS muss verantwortliche Stellen voneinander abschotten

Erschwert wird dies manchmal noch durch die Tatsache, dass ein Krankenhaus mit einem Medizinischem Versorgungszentrum (MVZ) oder verschiedenen Abteilung aus datenschutzrechtlich verschiedenen verantwortlichen Stellen bestehen kann, die aber alle gemeinsam einen Patienten behandeln wollen und daher Zugriff auf die entsprechende Patientendokumentation benötigen. Ein KIS muss also verantwortliche Stellen voneinander abschotten, aber auch gegenseitigen Zugriff ermöglichen können – je nach Fall.

Wie sollen nun solche Krankenhausinformationssysteme (KIS) gestaltet sein, dass sie sowohl den Anforderungen, die sich aus Datenschutz und der Schweigepflicht ergeben, als auch der guten Versorgung des Patienten – auch im Notfall – genügen? Was sind erforderliche, angemessene, dem Stand der Technik entsprechende technische und organisatorische Maßnahmen, um die gesetzlichen Anforderungen zu erfüllen?

Im März 2011 hat die 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zur datenschutzkonformen Gestaltung und Nutzung von Krankenhausinformationssystemen (OH KIS) verabschiedet.

Der AK Medizin des BvD hat bereits in seiner Stellungnahme vom Juni 2011 betont, dass er die OH KIS als Hilfe bei der Interpretation der gesetzlichen Vorgaben wie „zur Aufgabenerfüllung erforderlich“ und „Verhältnismäßigkeit“ sieht. Sie ist eine wertvolle Hilfe zur Unterstützung bei der Umsetzung von Maßnahmen beim Betreiber wie auch bei der Durchsetzung von Forderungen an die Hersteller. Sowohl Betreiber als auch Hersteller wurden durch die Diskussion, die seit Verabschiedung der OH

DATENSCHUTZTAGUNG 2013

Jahrestreff für Datenschutzbeauftragte und Datenschutzverantwortliche

Unternehmensberichte, Kurzseminare & Gruppen-Workshops

Ziel dieser Datenschutz-Jahrestagung ist es, mit Ihnen gemeinsam viele aktuelle Themen aus dem täglichen Arbeitsumfeld eines Datenschutzverantwortlichen in Form von Praxisberichten, Kurz-Seminaren und Gruppen-Workshops auszuarbeiteten, zu diskutieren und diese durch die Referenten mit Ergebnissen zu präsentieren. Die DASTAG bietet Ihnen am **gemeinsamen Abend** sowie am **DASTAG-Treff am Vorabend** ausreichend Zeit für viele Fachgespräche.

Auszug aus der Tagungsagenda der DASTAG – Unternehmensberichte, Kurzseminare & Workshops:

- ✓ **KEYNOTE:** Aufgaben & Befugnisse der Aufsichtsbehörden nach EU-Datenschutz-Grundverordnung
  Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Ansbach
- ✓ Datenschutz in der Wissenschaft - was Unternehmen lernen können / **Unternehmensbericht**
- ✓ Alltag eines Datenschutzbeauftragten im Technologie-Unternehmen / **Unternehmensbericht**
- ✓ Mobile Computing im Unternehmen mit Schwerpunkt BYOD / **Gruppen-Workshop**
- ✓ Allzeit gut abgesichert - Wenn die Aufsichtsbehörde klopft / **Kurzseminar**
- ✓ Selbstverteidigung für Datenschutzverantwortliche / **Kurzseminar**
- ✓ Datenschrank & Checklisten für den DSB / **Gruppen-Workshop**
- ✓ Beschäftigtendatenschutz / **Rechtlicher Vortrag**
- ✓ Datenschutz in sozialen Netzwerken / **Rechtlicher Vortrag**
- ✓ Notfallmanagement Datenschutz o. Live Hacking Cybercrime / **Praxisbericht Live Hacking**
- ✓ Datenschutz - von der Schulung zur Sensibilisierung / **Kurzseminar**

- ✓ **Kompaktes Wissen in 2 Tagen**
- ✓ **Business-Networking**
- ✓ **Sonderpreis für BvD-Mitglieder**
- ✓ **Teilnahme-Zertifikat**

Ausführliche **Tagungsagenda** und **Referenten-Profile** auf **www.dastag.de** / **Telefon: 089 4576918-12**

CBT Training & Consulting GmbH
www.cbt-training.de • www.it-secuta.de

KIS ins Rollen kam, für die Anforderungen, die an die Entwicklung und den Betrieb von KIS zu stellen sind, sensibilisiert.

Allerdings gibt es auch Probleme bei der Umsetzung der OH KIS: Eine integrierte oder fachabteilungsübergreifende Versorgung wird nur teilweise abgebildet. Einige Forderungen sind im Alltag schlecht oder nicht umsetzbar – entweder weil sie nicht praxisgerecht oder zu bürokratisch und unangemessen aufwändig sind. Teilweise stellen auch die Hersteller die Voraussetzungen nicht bereit, der Betreiber bleibt aber für die Umsetzung der datenschutzrechtlichen Vorgaben verantwortlich.

Intensive Diskussion unter rund 30 Datenschutzexperten

Über 30 Datenschutzbeauftragte aus kleinen und großen Krankenhäusern sowie Universitätskliniken, mehrere Vertreter der IT-Hersteller von Krankenhausinformationssystemen (KIS) und Leiter der Resorts „Gesundheit/Soziales“ von Datenschutzaufsichtsbehörden aus drei Bundesländern trafen sich am 25. September 2012 in Frankfurt zum „Workshop Orientierungshilfe KIS“ des AK Medizin des BvD.

Ziel des Workshops war das Gespräch zwischen Betreibern in den Kliniken, KIS-Herstellern und Datenschutzaufsichtsbehörden zu suchen. Viele Krankenhäuser haben einige Erfahrung mit der Umsetzung der OH KIS im eigenen Haus - teilweise zusammen mit den Aufsichtsbehörden - gesammelt. Vom gegenseitigen Erfahrungsaustausch können alle profitieren. Diese Erfahrungen sollten in einem Leitfaden zusammengefasst werden. Selbstverständlich sollten auch Probleme mit der OH KIS offen angesprochen und Änderungsvorschläge für die anstehende Überarbeitung der OH KIS formuliert werden.

- „Was ist bei der Umsetzung gut gelaufen?“
- „Wie setze ich die Anforderungen um und welche Anforderungen können erst mittelfristig oder nur mit Hilfe Dritter umgesetzt werden?“
- „Welche Anforderungen sind aus Sicht der Praktiker nicht umsetzbar?“

Unter diesen drei Fragestellungen griff der AK Medizin im Vorfeld vier Themen aus der OH KIS heraus, die in Arbeitsgruppen näher beleuchtet wurden.

Vorgehen zur Umsetzung der Orientierungshilfe: Die Arbeitsgruppe beschäftigte sich mit den Grundlagen, die notwendig sind, um die OH KIS umsetzen zu können. Eine Einbindung der Geschäftsführung, der Ärzte, der Pflegedienstleitung und auch des Betriebsrats ist unumgänglich. Externe Lieferanten des KIS oder der Komponenten des KIS müssen ebenfalls mit ins Boot geholt werden. Ob als Projekt oder nicht, ob mit externer Beratungsunterstützung oder ausschließlich intern – hier gab es unterschiedliche Erfahrungen der Teilnehmer.

Näher beleuchtet wurde auch die Rolle des Datenschutzbeauftragten bei der Umsetzung. Die Ergebnisse, Handlungsempfehlungen und Erfahrungsberichte sind in einem Leitfaden zusammengefasst.

Organisation des Einverständnisprozesses: Erforderliche Einwilligungen werden sinnvollerweise direkt bei der Aufnahme eingeholt. In der OH KIS wird zwischen administrativer und medizinischer Aufnahme unterschieden. Diese Unterscheidung ist im Alltag oft fließend und findet auch in verschiedener Reihenfolge statt. Dementsprechend wurde in der Arbeitsgruppe diskutiert, welche Aufgaben und Berechtigungen die administrative und medizinische Aufnahme benötigen.

Besondere Schwierigkeiten ergeben sich beim Umgang mit (Sperr-) Kennzeichen und dem Widerspruchsrecht. Die Arbeitsgruppe fasste ihre Erfahrungen in Handlungsempfehlungen zusammen. Dabei stellten sich auch konkrete Anforderungen an die Hersteller und Änderungsvorschläge an die OH KIS heraus.

Patienten wünschen sich eine Pseudonymisierung

Immer häufiger treten Patienten mit einem besonderen Schutzbedürfnis mit dem Wunsch nach Pseudonymisierung an die Betreiber heran. Leider war am Ende der Diskussion nicht mehr ausreichend Zeit, dieses Thema abschließend zu bearbeiten. Zusammen mit einem Vertreter der Hersteller besteht der Wunsch, die Anforderungen der Betreiber bei einer Pseudonymisierung zu konkretisieren. Diese Gespräche werden zwischen dem BvD und dem Bundesverband Gesundheits-IT zeitnah fortgeführt.

2B Secure

2B Advice bietet eine kostenlose uneingeschränkte Lizenz seiner Datenschutzlösung

- 2B Secure ist die Software-Gesamtlösung zur Organisation des betrieblichen Datenschutzes
- Alle zentralen Datenschutzprozesse im Griff – von der transparenten Analyse bis hin zur effizienten Umsetzung und lückenlosen Kontrolle aller aktuell gültigen Datenschutzbestimmungen

Bestellen Sie Ihre kostenlose Lizenz unter:
www.2b-advice.com

Zugriff auf Patientendaten im Rahmen der fachrichtungsübergreifenden Behandlung und von Funktionsstellen: Ein KIS ist nicht nur ein einziges System, sondern besteht aus vielen Systemen, die mit Schnittstellen miteinander verbunden sind. Die Interaktionen zwischen den Systemen finden häufig im Rahmen der fachrichtungsübergreifenden Behandlung statt. Schwerpunkt der Diskussion der Arbeitsgruppe war, wie die Berechtigungen entsprechend den Anforderungen der OH KIS bei den Schnittstellen konfiguriert werden können.

Kurz angesprochen wurde auch, wie innerhalb einer der Komponenten eines KIS die Berechtigungen v.a. beim fachrichtungsübergreifenden Zugriff gestaltet werden können. Enges Berechtigungskonzept in Kombination mit Protokollierung von Sonderzugriffen ist eine Möglichkeit. Auch dieses Thema konnte aus Zeitgründen leider nicht vertieft werden. Hierzu wird der AK Medizin den Leitfaden entwickeln.

Möglichkeiten und Grenzen der geforderten Protokollierung und Kontrolle von Zugriffen auf Patientendaten: Jeder Patient hat das Recht zu erfahren, wer auf seine Daten zugegriffen hat. Wenn Sonderzugriffe außerhalb eines systemseitig festgestellten Behandlungsauftrags im KIS (oder einer Teilkomponente des KIS) und außerhalb der standardmäßig vergebenen Berechtigungen erfolgen, müssen diese protokolliert werden.

Umfang der Protokollierung und die Auswertung waren Thema der Arbeitsgruppe. Hier ist der KIS-Betreiber häufig auf die Unterstützung des Herstellers angewiesen. Beim Betreiber selbst muss geklärt werden, wer zu welchem Zweck und in welchem Umfang die Kontrollen durchführt. Diskutiert wurde vor allem über die sich aus der OH KIS ergebenden Anforderungen, welche Zugriffe überhaupt zu protokollieren sind und wie die der Auswertung der protokollierten Daten erfolgen soll und darf. Grundsätzlich ist die Zugriffsprotokollierung dem Recht des Patienten auf Auskunft und der Datenschutzkontrolle zur Feststellung berechtigter oder unberechtigter Zugriffe auf Patientendaten geschuldet. Es muss also anhand der Protokolldaten feststellbar sein, wer wann zu welchen Zwecken auf welchen Patienten zugegriffen hat. Protokolldaten sind nicht mit den zur Eingabekontrolle erfolgten Datenbankeinträgen zu verwechseln, auch wenn diese vor allem bei schreibenden Zugriffen (z.B. Arztbriefschreibung, Befundvalidierung, Dokumentation erfolgter Behandlung und Diagnostik) häufig zur Protokollierung der Zugriffen verwendet werden.

Betreiber, Hersteller und Aufsichtsbehörden diskutierten offen und konstruktiv die Anforderungen, die sich aus der OH KIS ergeben. Die anwesenden Vertreter der Aufsichtsbehörden sahen die OH KIS nicht als Checkliste, um sofort danach Beanstandungen auszusprechen, sondern eher als Diskussionsgrundlage für einen konstruktiven Dialog mit den Betreibern. Da die Betreiber auf die Voraussetzungen in den KIS-Anwendungen, die ihnen die Hersteller zur Verfügung stellen, angewiesen sind, war der Workshop eine gute Gelegenheit, im Dialog miteinander Wünsche der Betreiber und technische Möglichkeiten der Hersteller anzusprechen.

Die Gespräche werden intensiv fortgeführt

Mehrere Ziele des Workshops wurden erreicht:

- Betreiber, Hersteller und Aufsichtsbehörden sind im Dialog, um gemeinsam Krankenhausinformationssysteme so zu gestalten, dass die Persönlichkeitsrechte der Patienten besser gewahrt werden können.
- Wünsche zu Verbesserungen sowohl bei der OH KIS als auch bei der Gestaltung der KIS durch die Hersteller wurden offen formuliert.
- Jede Arbeitsgruppe hat Fragen diskutiert und Handlungsempfehlungen für die Umsetzung der OH KIS erstellt.
- Alle Teilnehmer konnten vom gegenseitigen Erfahrungsaustausch profitieren.

Handlungsleitfaden, Anforderungen an Hersteller und Änderungen bei der OH KIS bzw. Unterstützung durch die Aufsichtsbehörden sind als Ergebnis des Workshops zusammengefasst. Das Ergebnis wurde allen Teilnehmern sowie den Aufsichtsbehörden und dem bvitg zur Verfügung gestellt.

Die Gespräche insbesondere zwischen uns Datenschutzbeauftragten als Vertreter der Betreiber und dem bvitg als Verband der Hersteller werden intensiv fortgeführt.

Autorin

Barbara Stöferle
Ansprechpartnerin
AK Medizin
E-Mail: ak-medizin@bvdnet.de

AK Sozial etabliert sich

„Datenschutz in sozialen Einrichtungen“ weckt großes Interesse

Bereits zum 5. Arbeitstreffen hatte sich der Arbeitskreis am 17. Januar 2013 in Fulda in den Räumen der Regionalgeschäftsstelle der PARITÄTISCHE Hessen zusammengefunden. Im Schnitt treffen sich von den 13 gemeldeten Mitgliedern des Arbeitskreises neun bis elf aktive Teilnehmer.

In der 4. Sitzung war eine Vertreterin der Bundesvereinigung Lebenshilfe e.V. aus Berlin eingeladen. Ricarda Langer berichtete über eine im letzten Sommer durchgeführte Umfrage bei Trägern von Einrichtungen und Diensten der eigenständigen Lebenshilfe-Vereine und Werkstätten. Der Präsentation der Ergebnisse folgten Diskussionen innerhalb des Arbeitskreises über die Umsetzung des Datenschutzes in der täglichen Praxis. Abschließend bot Ricarda Langer an, Fachbeiträge des Arbeitskreises in der geplanten Datenschutzbroschüre der Bundesvereinigung aufzunehmen. Aktuell läuft dazu die Bewertung der AK-Beiträge durch die Redaktionsgruppe der Lebenshilfe. Für die 6. Sitzung des Arbeitskreises am 18. April bei der Lebenshilfe Gießen sind die Mitglieder aufgefordert, Ergebnisse und Übersichten am Beispiel „rechtssichere Begriffe“ aus ihren Tätigkeits- und Betreuungsumfeldern aufzuarbeiten. Zudem ist eine Präsentation zum Thema „Schweigepflichtentbindung“ vorgesehen. Weiter werden Gäste aus dem Bereich der Behindertenhilfe und einem Anbieter der Jugend-, Sozial- und Bildungsarbeit erwartet. Insgesamt gewinnt der Arbeitskreis durch die Vielfalt der durch die AK-Mitglieder betreuten sozialen Einrichtungen. Der Meinungs- und Informationsaustausch untereinander, auch außerhalb der regulären Sitzungen, ist eine Bereicherung in der täglichen Arbeit gerade in sozialen Bereichen mit seinen vielfältigen Datenschutzfacetten.

Autorin

Ilse Römer
Ansprechpartnerin
AK Sozial
E-Mail: ak-sozial@bvdnet.de

RHENUS LOGISTICS

MOBILE AKTENVERNICHTUNG

Sicherheit, die zu Ihnen kommt

VOM DATENSCHUTZ EMPFOHLEN*

Prüf-Nr.: 04-08 / 2009
Befristet bis 6. November 2014

Maximale Sicherheit für Ihre Akten und Datenträger

Lassen Sie sich von unserer vollständig offenbarungsfreien und ordnungsgemäßen mobilen Vernichtung Ihrer Daten nach DIN 66399 überzeugen.

Unsere mobile Aktenvernichtung ist mit dem Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zertifiziert.

Wir sind gern für Sie da. Kontaktieren Sie uns.

Rhenus Data Office GmbH · Industriestraße 5 · 48301 Nottuln
Telefon: +49 (0)800 988 5 988 · info.data-office@de.rhenus.com · www.aktenvernichtung.de

AK Social Media – Ein Arbeitskreis stellt sich vor

Arbeitskreis will BvD-Mitglieder aktiv im Umgang mit Social Media unterstützen: durch Arbeitsmaterialien, Fortbildungen und mehr

Stefan Bachmann

Juliane Billhardt

Robert Eppli

Sven Henze

Christoph Heyn

Frank Spaeing

Informationelle Selbstbestimmung ist und bleibt auch in Zeiten der sozialen Vernetzung einer der elementarsten Grundsätze. Das Recht von Individuen selbst zu bestimmen, wem seine Gedanken, Gefühle und Meinungen mitgeteilt werden, wird mit Web 2.0 Technologien wichtiger denn je. Aber auch unüberschaubarer für den Einzelnen wie auch für Unternehmen. Umso bedeutsamer wird es für den Verband eine Stimme zu bekommen, die auch die Social Media Sprache spricht.

In der zweiten Jahreshälfte 2012 ist der BvD einen weiteren Schritt in diese Richtung gegangen. Ein neuer Arbeitskreis wurde gebildet, der als Schwerpunktthemen unter anderem die Außenwirkung des BvD bei der Diskussion rund um neue Technologien verbessern und zudem das Schulungs- und Informationsangebot für BvD-Mitglieder erweitern soll.

AK social Media als Sprachrohr: Eine elementare Möglichkeit, Außenwirkung zu gestalten, ist ein gegenwartsnaher Auftritt im wohl bekanntesten Online-Lexikon Wikipedia. Eine Teilaufgabe, die durch den neuen Arbeitskreis bereits umgesetzt wird.

Seminar thematisiert Facebook für Datenschutzbeauftragte

Fort- und Weiterbildung: „Soziale Netzwerke in Unternehmen" war der Titel eines Seminars, das im November 2012 von zwei Mitgliedern des Arbeitskreises durchgeführt wurde. Eine zweite Veranstaltung ist für den 24. April 2013 in Berlin terminiert: „Facebook für Datenschutzbeauftragte". Auch in Zukunft werden aus dem Arbeitskreis Social Media heraus weitere Themen für mögliche BvD-Seminare entwickelt werden.

Folgende Projekte stehen auf der Agenda des Arbeitskreises:

Blog: Eine Option, News schnell an interessierte Nutzer zu verbreiten, ist die Installation eines Blog. Zusätzlich zur Veröffentlichung von aktuellen Informationen wird eine Diskussionsplattform etabliert, die den zentralen Austausch von Meinungen ermöglicht und somit für eine große Anzahl von Nutzern eine Bereicherung sein wird. Dieses Thema wird vom Arbeitskreis begleitet.

Arbeitsmaterialien für BvD-Mitglieder: Eines der selbstgesteckten Ziele des Arbeitskreises ist es, Kommentierungen, Beschreibungen sowie Unterlagen für die Beratung im Umgang mit sozialen Technologien bereitzustellen.

Wie können soziale Plattformen sicher genutzt werden?

Datenschutzkonforme Social Media Technologien: Zu bekannten Plattformen wie Twitter, Facebook gibt es meist datenschutzverträgliche Alternativen. Der Arbeitskreis will Einblicke und Hintergründe zu diesen Plattformen ermöglichen.

Web 2.0 Werkzeuge: Datenschutzbeauftragte sind nach §4g BDSG verpflichtet, auf die Einhaltung des Datenschutzes hinzuwirken. Ist eine soziale Plattform in einem Unternehmen etabliert, sind Möglichkeiten gefragt, über Tools und Anwendungen die Nutzung der Plattformen so sicher wie möglich zu gestalten.

Der Arbeitskreis setzt sich zusammen aus der Sprecherin Juliane Billhardt, ihrem Stellvertreter Sven Henze, Stefan Bachmann, Robert Eppli, Christoph Heyn und Frank Spaeing.

Evaluation von § 30a und § 42a BDSG durch Bundesregierung

Die wichtigsten Details aus dem eingeforderten Bericht

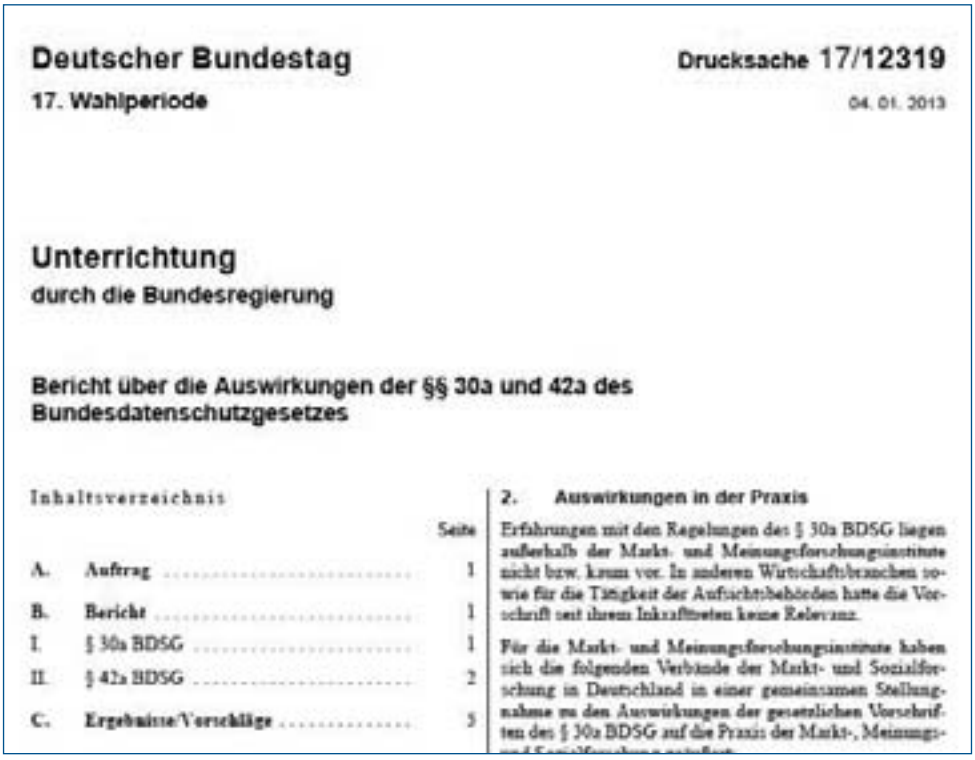
Im Rahmen der BDSG Novelle II 2009 wurden durch den Gesetzgeber zwei neue Vorschriften eingefügt, über deren Auswirkungen die Bundesregierung dem Bundestag bis 31.12.2012 gemäß § 48 BDSG berichten sollte. Gleichzeitig wurde der Bundesregierung auferlegt, bei Änderungswünschen entsprechende Vorschläge vorzulegen. Dieser Bericht liegt nun vor (vgl. Bundestagsdrucksache 17/12319, http://www.bundestag.de/presse/hib/2013_03/2013_125/02.html) und wurde am 7.3.2013 veröffentlicht.

Im Ergebnis sieht die Bundesregierung weder bei § 30a BDSG (Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung) noch bei § 42a BDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten) Handlungsbedarf. In dem Bericht (http://dip21.bundestag.de/dip21/btd/17/123/1712319.pdf) legt die Bundesregierung dar, dass der § 30a BDSG seinen Platz zwischen der eigenen-Marktforschung durch Unternehmen nach § 28 BDSG sowie der wissenschaftlichen Forschung nach § 40 BDSG finde. Abgrenzungsprobleme zwischen diesen Bereichen sind nach Auffassung der Bundesregierung Fragestellungen, die typischerweise mit der Anwendung abstrakter Normen in der Praxis einhergehen.

Soweit im Rahmen der Evaluation auch die Hintergründe der Meldungen geschildert wurden, clustert der Bericht folgende typischen Fälle:

- Verlust (Diebstahl, Abhandenkommen) von Hardware (USB-Stick/Laptop/Notebook)
- Falscher Versand/Verlust von Dokumenten mit personenbezogenen Daten (z. B. Bankunterlagen wie Kontoauszüge etc.)
- Unberechtigter Zugriff auf Webserver/Erschleichen von Daten

In dem Berichtsteil, der sich dem § 42a BDSG widmet, werden zunächst die Historischen dargestellt. Interessant ist eine Auflistung der bis zum 31.12.2012 bei den Aufsichtsbehörden gemeldeten



Deutscher Bundestag **Drucksache 17/12319**

17. Wahlperiode 04. 01. 2013

Unterrichtung
durch die Bundesregierung

Bericht über die Auswirkungen der §§ 30a und 42a des Bundesdatenschutzgesetzes

Inhaltsverzeichnis

		Seite
A.	Auftrag	1
B.	Bericht	1
I.	§ 30a BDSG	1
II.	§ 42a BDSG	2
C.	Ergebnisse/Vorschläge	5

2. Auswirkungen in der Praxis

Erfahrungen mit den Regelungen des § 30a BDSG liegen außerhalb der Markt- und Meinungsforschungsinstitute nicht bzw. kaum vor. In anderen Wirtschaftsbranchen sowie für die Tätigkeit der Aufsichtsbehörden hatte die Vorschrift seit ihrem Inkrafttreten keine Relevanz.

Für die Markt- und Meinungsforschungsinstitute haben sich die folgenden Verbände der Markt- und Sozialforschung in Deutschland in einer gemeinsamen Stellungnahme zu den Auswirkungen der gesetzlichen Vorschriften des § 30a BDSG auf die Praxis der Markt-, Meinungs-

Fälle. So wurde bei insgesamt 305 Meldungen die Tatbestandsvoraussetzungen des § 42a BDSG in 177 Fällen bejaht, jedoch nicht ohne darauf hinzuweisen, dass aufgrund der völligen Unabhängigkeit der Aufsichtsbehörden diese Subsumierung nicht überprüft wurde.

Anmerkungen der Aufsichtsbehörden: Ergänzt wird der Bericht durch Anmerkungen der Aufsichtsbehörden und der Stellungnahmen der Bundesregierung dazu. So wird beispielsweise bezüglich der Anmerkung des Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI) Nordrhein-Westfalen, dass zweifelhaft sei, ob auch ein Dritter, stellvertretend für den Benachrichtigungspflichtigen, der Informationspflicht nachkommen könne (z. B. Versicherung stellvertretend für selbständige Makler) durch die Bundesregierung darauf hingewiesen, dass nicht erkennbar ist, warum bei den in § 42a BDSG erforderlichen Meldungen die Stellvertretungsregelungen nicht gelten sollten.

Den Anmerkungen des Landesbeauftragten für Datenschutz und Informationsfreiheit Bremen und des Bayerischen Landesamt für Datenschutzaufsicht (denen sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit anschloss) zufolge sollte § 42a Satz 1, 2. Alt. BDSG in der Weise klar gestellt werden, dass es genüge, wenn die verantwortliche Stelle feststellt, dass die Daten Dritten unrechtmäßig zur Kenntnis gelangt sein können. Das Abstellen auf die Tatbestandsvoraussetzung, dass die speichernde Stelle feststellt, dass die Daten Dritten zur Kenntnis gelangt sind, sei zu eng und führe in der Praxis zu Diskussionen.

Die Bundesregierung sieht in dem Bericht (dort Ziffer II 4.b) auch hierzu keinen Änderungsbedarf. Sie verweist auf Kommentarstellen in der Literatur, dass eine Meldepflicht nur bestehe, wenn eine Kenntniserlangung mit hoher Wahrscheinlichkeit vorliegt (z. B. Dix, in: Simitis, BDSG, § 42a RNdnr. 8). Anderenfalls müsse jede folgenlose Unachtsamkeit gemeldet werden. Dies würde ver-

DATENSCHUTZ | SAP SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

Die gesetzlichen Anforderungen erfüllen – und mehr
Praxisorientierte Umsetzung

> Datenschutzanalyse
> Konzerninterner Datenverkehr
> Auftragsdatenverarbeitung – Datenschutz in der Cloud
> SAP HCM Datenschutz-Audit
> Datenschutz in den Sozialen Medien
> Onlinebewerbermanagement

Anerkannte Sachverständige und Prüfstelle für Recht und Technik beim ULD für das Datenschutz-Gütesiegel

ditis Systeme – Niederlassung der JMV GmbH & Co. KG Heidenheim • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 13 • 89081 Ulm • Tel +49 731 509704 - 40 • E-Mail info@ditis.de • www.ditis.de

Über die Auswirkungen zweier neuer Vorschriften im Rahmen der BDSG Novelle II 2009 informierte die Bundesregierung den Bundestag. (Foto: Deutscher Bundestag / Marc-Steffen Unger)

kennen, dass die Norm keine umfassende Pflicht zur Selbstanzeige oder eine Bestrafung für Unachtsamkeit zum Ziel hat, sondern Schaden vom Betroffenen abwenden und die Verantwortlichen zu einer stärkeren Wahrnehmung ihrer Verantwortung veranlassen will.

Ferner wird ausgeführt, dass die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen (der sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit anschließt) kritisierte, dass neben der Tatsache des Abhandenkommens von Daten auch noch gefordert werde, dass aus dem Abhandenkommen Beeinträchtigungen drohen und diese schwerwiegender Art sein müssen. Sie empfehle, diese Voraussetzungen zu streichen. Auch hier sieht die Bundesregierung keinen Änderungsbedarf. § 42a BDSG beinhaltet durch die Pflicht zur Selbstoffenbarung und Selbstanzeige einen nicht unerheblichen Eingriff in die Grundrechte der verantwortlichen Stelle. Dieser ist nur zu rechtfertigen, wenn auf der Seite des Betroffenen ebenfalls ein erheblicher Eingriff droht oder stattgefunden hat, selbst wenn eine solche Beeinträchtigung bei sensiblen Daten besonders wahrscheinlich ist (Bericht Ziffer II 4 c).

Desweiteren sind in dem Bericht auch Ausführungen zu den Stellungnahmen von Verbänden dargelegt und durch die Bundesregierung teilweise auch bewertet.

Leider lässt der Bericht Ausführungen zu den Problemen durch Informationsfreiheitsgesetze vermissen: In den Bundesländern, in denen über ein Informationsfreiheitsgesetz die Öffentlichkeit bzw. die Presse einen gesetzlichen Anspruch auf Einsicht/Auskunft in Verwaltungsvorgänge hat, muss auch das Unternehmen, welches eine vermeintliche Datenpanne meldet, damit rechnen, dass diese Anfrage an die Öffentlichkeit gerät. Dies selbst dann, wenn die Aufsichtsbehörde ein erforderliches Tatbestandmerkmal nach § 42a BDSG verneint. Angesichts der Pflicht zur Selbstanzeige sicherlich ein Umstand, der bei Zweifeln der Unternehmen eine Anfrage bei den Aufsichtsbehörde nicht fördern wird. Das Fehlen dieser Thematik in den Stellungnahmen der Aufsichtsbehörden lässt sich nur damit erklären, dass diese Zusammenhänge offensichtlich erst nach Meldung der Erfahrungen zu § 42a BDSG durch die Aufsichtsbehörden gegenüber der Bundesregierung ins Bewusstsein der Aufsichtsbehörden gelangte.

Autor

Rudi Kramer
Rechtsanwalt,
Datenschutzreferent bei der DATEV eG
BvD-Vorstand

Datenschutz auf dem Social Learning Summit 13

Ein Erfahrungsbericht von BvD-Vorstandsmitglied Thomas Floß

In der Eigenschaft als BvD -orstandsmitglied und als einer der Datenschutzexperten in Sachen Social Media war ich zum Social Learning Summit 13 in Berlin am 18. Januar von der Stiftung „Digitale Medien“ eingeladen.

Neben weiteren hochrangigen Experten – darunter Thilo Weichert vom ULD Schleswig Holtstein, Eva-Maria Kirschsieper von Facebook und Prof. Dr. Nadia Kutscher von der Katholischen Hochschule in NRW – saßen wir mit einem halben Duzend Jugendlichen aus der ersten (Alter 13-20 Jahre) und zweiten (Alter: 21-27 Jahre) „Digital Natives-Generation“ in der Arbeitsgruppe „Social Media und Datenschutz“. Neben dieser Gruppe gab es noch weitere Workgroups zu Themen wie „Identität & Inzenierung“, „Social Media@Family“, „Social Media@School“ sowie „Gefährdung und Hilfe“.

Zwei verschiedene Generationen, zwei verschiedene Sichtweisen

Nach kurzer Vorstellung der Runde wurden die Kids (Jahrgangsstufe 8) und jungen Erwachsene nach ihrem Nutzungsverhalten in Facebook befragt. Bis auf ein Mädchen (13 Jahre) waren alle Online, hatten aber laut eigener Aussage ihre Profile gut geschützt. Dieses ist nach den Erfahrungen des Arbeitskreises „Datenschutz geht zur Schule“ nicht die Regel: In der Praxis sieht das leider häufig ganz anders aus. Weiterhin sind alle derzeit mit ihrem echten Namen registriert. Das wollten wir doch genauer wissen und fragten hier noch einmal nach. Die Antwort, erstaunlich aber doch einfach: „Man will doch gefunden werden“.

Sehr interessant und vollkommen neu waren für mich die Aussagen zu Freundschaftsanfragen innerhalb Facebooks. Hier sagten die Jugendlichen der zweiten Facebookgeneration übereinstimmend, dass es doch sehr unhöflich sei, eine Freundschaftsanfrage abzulehnen. Dieses ergibt ein vollkommen neues Bild in Bezug auf das Nutzungsverhalten. Das erklärt auch weiterhin, warum die Jugendlichen die Freundschaftsanfragen bei unseren Vorfeldrecherchen zu den Unterrichtseinheiten sehr häufig annehmen. Resümee: Lesson Learned, ich habe verstanden!

Für die Jüngeren ist Vertrauen untereinander wichtiges Thema

Dieses steht jedoch im krassen Gegensatz zur ersten Generation. Hier werden Freundschaftsanfragen grundsätzlich nur angenommen, wenn die Anfragenden auch persönlich bekannt sind. Das erste Facebook-Generationenproblem?

Nach dem Vertrauen in Bezug auf Freunde und Facebook befragt, ergibt sich ebenfalls ein vollkommen differenziertes Bild. Die zweite Facebookgeneration macht sich in Bezug auf die Sicherheit der Anbieterplattform (Facebook, Google+) keinerlei Gedanken, nach dem Motto „passt schon“. Die erste Facebookgeneration ist hier deutlich misstrauischer, sie wissen oder meinen zu wissen, was passiert (Werbung, Weitergabe der Daten etc.) und sind hier mit der Preisgabe ihrer persönlichen Daten erheblich sensibler.

Für die Jüngeren ist das Vertrauen untereinander dagegen viel wichtiger. Man spricht hier ab, ob ein Bild online gestellt werden darf oder nicht. Ich halte diese Aussage allerdings nicht für repräsentativ, aber dennoch für extrem wichtig. Auch hier wieder: Lesson Learned, ich habe verstanden. Nach den Wünschen an z.B. Facebook gefragt, sagten die jungen Damen, dass die AGBs einfacher sein müssen. „Wer liest schon 12 Seiten und versteht die auch noch?“ Die Kids wünschen sich einfache und altersmäßg verständliche AGBs, @Facebook: Lesson Learned?

Abschließend wurden alle Ergebnisse der Arbeitsgruppen im Podium von rund 150 Teilnehmern vorgetragen und auch diskutiert. Auch das

Autor

Thomas Floß
ist BvD-Vorstandsmitglied und hier verantwortlich für die Initiative „Datenschutz geht zur Schule“

Podium war von unseren Ergebnissen durchaus überrascht. Besonders die Aussage nach dem hier doch so vernünftig dargestellten Verhalten bei dem Upload von Fotos löste Verwunderung aus. Von einer Teilnehmerin wurden die Schülerinnen dann gefragt, ob sie eine Idee hätten, warum denn so viele andere ihres Alters Bilder häufig ohne Sinn und Verstand hochladen würden. Die Antwort der Schülerin, einfach wie genial: „Manchmal ist das Handy halt schneller als der Kopf". Vor dieser jungen Lady ziehe ich meinen Hut, denn sie hat mit ihren 13 oder 14 Jahren den Nagel auf den Kopf getroffen.

Treffen mit Facebook-Vertreter in Versmold geplant

Abschließend habe ich noch Facebook in die Pflicht genommen und an Dr. Bender (zuständig für den Bereich Datenschutz in Deutschland) gerichtet gesagt, dass ich nun erwarten würde, dass die hier aufgezeigten Vorschläge auch umgesetzt werden. Weiterhin habe ich die Hilfe des BvD angeboten. Die Dozenten der Initiative sind doch fast täglich im Feld und hören, wo der Schuh drückt. Dr. Bender und Team haben zugesagt, sich die Problem und Nöte anzuhören und auch darauf zu reagieren.

Hier steht nun der BvD mit seinem Dozententeam in der Pflicht, die Probleme und Anregungen an mich oder die Geschäftsstelle weiterzuleiten. Vielleicht können wir ja dazu beitragen, Facebook ein wenig anwenderfreundlicher zu machen. Und, es wurde ein erstes Treffen mit Dr. Bender von Facebook vereinbart, und das auch noch in der Weltstadt Versmold :-).

Letztendlich muss ich sagen, dass es eine sehr gelungene Veranstaltung war. Man kann wirklich sagen: viel gelernt. Die Fahrt nach Berlin hat sich also wirklich gelohnt und ich bin sicher, dass wir in Bezug auf den Datenschutz bei Facebook weiterkommen werden. Wie schnell und welchem Umfang, das wird dann natürlich erst die Zukunft zeigen können.

BvD-Vorstand Thomas Floß war für den Verband in Berlin zu Gast bei der Stiftung „Digitale Medien" beim Social Learning Summit 13.

Datenschutz für Facebook-Nachrichten

Simon Rothe entwickelt ein Browser Add-on, das mit der Website der Social Media-Plattform interagiert

Soziale Netzwerke, insbesondere Facebook, erfreuen sich immer größerer Beliebtheit. Durch alle Altersgruppen hinweg werden sie immer stärker genutzt und haben die Tendenz Kommunikationsplattform Nummer Eins des Internets zu werden.

Es ist einfach sehr komfortabel sich über Neuigkeiten aus seinem Freundeskreis zu informieren und zusätzlich die Möglichkeit zu haben seine Freunde direkt zu kontaktieren. Doch leider scheint der Datenschutz dabei ins Hintertreffen zu gelangen. Das aus den USA stammende Unternehmen Facebook operiert offensichtlich auch in Europa unter den für uns nicht genügend weitreichenden amerikanischen Datenschutzrichtlinien. Daher beurteilte der Hamburger Datenschutzbeauftragte Thilo Weichert Facebooks Vorgehen in Deutschland und Europa als illegal [vergleiche dazu den Beitrag im Internet unter der Adresse www.theeuropean.de/thilo-weichert/11075-facebooks-umgang-mit-benutzerdaten].

Sicherheit in der Facebook-Kommunikation: Mit PrivKey werden Nachrichten auf der Social Media-Plattform verschlüsselt übertragen.

Mein Name ist Simon Rothe. Derzeit absolviere ich ein duales Studium beim Deutschen Zentrum für Luft- und Raumfahrt (Informationstechnik). Aus persönlicher Erfahrung während eines Freiwilligen Sozialen Jahres in Südafrika weiß ich, wie bedeutend es ist sichere und vertrauensvolle Kommunikationskanäle zu haben. Stellen Sie sich vor, Ihr Chef könnte alles Lesen, was Sie jemals von sich gegeben haben. Daher habe ich mich nach vorzeitigem Beenden eines Physik-Studiums daran gesetzt PrivKey zu entwickeln. PrivKey ist ein Browser Add-on für Firefox und Chrome. Es interagiert mit der Facebook-Website; kurz bevor Sie eine Nachricht versenden wird sie vom Add-on aufgegriffen und dann verschlüsselt an den Facebook-Server versandt – Sobald auf der Website eine verschlüsselte Nachricht erscheint, wird diese vom Add-on detektiert und mit entsprechender Kennzeichnung entschlüsselt dargestellt.

Die Nachrichten werden also wie bisher über Facebook versandt, nur dass sie nicht im Klartext sondern verschlüsselt übertragen werden. Als Verschlüsselungsstandard wird OpenPGP verwandt, wie er für sichere E-Mail-Kommunikation bereits etabliert ist. Durch die Verwendung des Standards ist eine Erweiterbarkeit und Kompatibilität über andere Anwendungen hinweg gegeben.

Ich weiß nicht in wie weit Sie Facebooks Nachrichtendienst privat oder auch im Umfeld Ihres Unternehmens nutzen. Aber Sie sollten sich in jedem Fall fragen, in wie weit Sie damit übereinstimmen, dass Ihre vertrauliche Kommunikation, für die wir aus alten Zeiten das Briefgeheimnis kannten, für immer gespeichert bleibt, automatisch ausgewertet wird und Sie damit zu einer transparenten und steuerbaren Person macht.

Für weitergehende Recherche über das Potenzial von Facebooks Datenschutzverletzungen bietet der Wikipedia-Artikel Facebook (Abschnitt Kritik) einen guter Einstiegspunkt (http://de.wikipedia.org/wiki/Facebook#Kritik). PrivKey finden Sie unter http://www.PrivKey.de oder über die eigene Facebook-Fanpage: http://www.facebook.com/PrivKey.

Es ist eine ständige Herausforderung PrivKey so zu entwickeln, dass es sich möglichst intelligent an die sich fortwährend ändernde Facebook-Website adaptiert. Auch die Entwicklung neuer Features, so wie Promotiontätigkeiten neben den Belastungen des Studiums erfordern ausdauernden Einsatz. Geplant ist zudem eine Version für mobile Endgeräte (Smartphones).

Wenn Sie mein Vorhaben für unterstützenswert halten, oder sich angesprochen fühlen einen kleinen Beitrag zu leisten, dann lassen Sie es mich wissen!

Autor

Simon Rothe
Archenholzstr. 12
22117 Hamburg
Tel: 040 / 732 83 16
E-Mail: info@privkey.de
Internet: www.privkey.de

MARKUS SCHRÖDER

Arbeitnehmerdatenschutz beim Fleetmanagement

Mitbestimmungspflichtigkeit bei der Datenübermittlung?

Auftragsdatenverarbeitung
Arbeitnehmerüberwachung
Mitbestimmung
Anonymisierung von Arbeitnehmerdaten

■ Die Vergabe von Firmenwagen hat für Unternehmen eine große wirtschaftliche Bedeutung. Außendienstmitarbeiter sind auf sie angewiesen. Leitende Mitarbeiter erhalten Firmenwagen regelmäßig als Teil ihres Vergütungspakets und zur Repräsentanz des Unternehmens. Zumeist wird das Fuhrparkmanagement an Konzerngesellschaften oder externe Anbieter ausgegliedert. Bei diesen Konstellationen sind jedoch datenschutzrechtliche Voraussetzungen zu beachten, da zwangsläufig Arbeitnehmerdaten verarbeitet werden.

■ Granting business cars is of great economic importance for companies. Field staff are dependent upon them. Managerial staff regularly are granted business cars as part of their remuneration package and to represent the company. Generally, the management of the fleet is outsourced to affiliated companies or external service providers. However, in these setups, data protection law requirements must be observed as employee data is inevitably processed.

I. Einleitung

Das Fuhrparkmanagement ist für Unternehmen von besonderer Bedeutung. Zunächst in rein wirtschaftlicher Hinsicht. So werden Mitarbeitern Dienstwagen häufig als Teil ihres Vergütungspakets zur Verfügung gestellt. Zudem sind Außendienstmitarbeiter bei ihrer Tätigkeit auf ein Fahrzeug angewiesen. Herausforderungen für die Unternehmen bestehen beim Fuhrparkmanagement jedoch auch in rechtlicher – insbesondere in datenschutzrechtlicher – Hinsicht. Die datenschutzrechtlichen Fragen beim Betrieb eines Fuhrparks dürfen nicht unterschätzt werden. So verhängte kürzlich der *Hamburgische Datenschutzbeauftragte* ein Bußgeld i.H.v. € 54.000,– gegen die Autovermietung *Europcar*, weil diese einen Teil ihrer Flotte ohne Wissen der Mieter per GPS hatte orten lassen.[1]

II. Rechtsfragen

1. Auftragsdatenverarbeitung

Üblicherweise wird das Fleetmanagement an eine eigens zu diesem Zweck gegründete Konzerngesellschaft oder an einen Drittanbieter ausgegliedert. Zwischen der ausgliedernden Gesellschaft und dem Flottenmanagementbetreiber ist regelmäßig eine Auftragsdatenverarbeitung gegeben, wobei die ausgliedernde Gesellschaft Auftraggeber und der Flottenmanagementbetreiber Auftragnehmer ist. Grenzt man die Auftragsdatenverarbeitung zur sog. Funktionsübertragung ab, so liegt eine Auftragsdatenverarbeitung nur dann vor, wenn der Auftragnehmer dem Auftraggeber gegenüber weisungsabhängig bei der Datenverarbeitung ist und lediglich eine Hilfsfunktion wahrnimmt.[2] Die von dem Flottenmanagementbetreiber erbrachten Tätigkeiten sind regelmäßig streng weisungsabhängig definiert und stellen ebenfalls regelmäßig eine reine Hilfsfunktion für die eigentlichen Geschäftszwecke des Auftraggebers dar. Daher liegt hier im Regelfall schon i.S.d. Funktionsübertragungstheorie eine Auftragsdatenverarbeitung vor.

Gänzlich problemlos ist i.S.d. Vertragstheorie eine Auftragsdatenverarbeitung gegeben. Entscheidend kommt es nach der Vertragstheorie darauf an, dass ein den Voraussetzungen des § 11 BDSG entsprechender Vertrag zwischen Auftraggeber und Auftragnehmer vorliegt.[3] Da – wie schon zur Funktionsübertragungstheorie gesagt – ein mit einem Flottenmanagementbetreiber geschlossener Vertrag üblicherweise eng definierte Weisungen für die Datenverarbeitung enthält, können die Parteien durch eine entsprechende Vertragsgestaltung die Voraussetzungen einer Auftragsdatenverarbeitung erfüllen. Daher sollte in jedem Falle besonderes Augenmerk auf die Vertragsgestaltung gelegt werden.

2. Führerscheinüberprüfung gem. § 21 Abs. 1 Nr. 2 StVG

Für das Unternehmen ist weiterhin zu bedenken, dass es die Halterpflichten des Straßenverkehrsrechts treffen. So macht sich gem. § 21 Abs. 1 Nr. 2 StVG der Fahrzeughalter strafbar, der vorsätzlich oder fahrlässig anordnet oder zulässt, dass jemand das Fahrzeug führt, der keine Fahrerlaubnis hat oder gegen den ein Fahrverbot besteht. Um diesen Sorgfaltspflichten zu entsprechen, muss der Halter sich durch Einsicht in den Führerschein davon überzeugen, dass der Fahrzeugführer im Besitz der einschlägigen Fahrerlaubnis ist.[4] Demnach muss das Unternehmen als Halter der Flottenfahrzeuge die Führerscheine derjenigen Mitarbeiter einsehen, die einen Firmenwagen nutzen sollen. Es stellt sich nun die Frage der datenschutzrechtlichen Zulässigkeit der in diesem Zusammenhang erfolgenden Datenverarbeitung. Zu denken ist zunächst an die Unterzeichnung einer Einwilligungserklärung durch die entsprechenden Mitarbeiter. Allerdings tritt hierbei das Problem auf, dass Einwilligungserklärungen durch die Arbeitnehmer in einem Arbeitsverhältnis unwirksam sein könnten.[5]

Im Sinne der Rechtssicherheit sollten daher die ergriffenen Maßnahmen auf gesetzlicher Grundlage legitimiert sein. Zu denken ist dabei zunächst an den Erlaubnistatbestand des § 32 Abs. 1 Satz 1 BDSG. Demnach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Jedenfalls bei Außendienstmitarbeitern oder Berufskraftfahrern ist die zur Durchführung der Führerscheinüberprüfung erforderliche Datenverarbeitung durch § 32 Abs. 1 Satz 1 BDSG legitimiert, da der Beschäftigte seine Tätigkeit nicht ausüben kann, ohne im Besitz einer Fahrerlaubnis zu sein. Daher ist die Kontrolle des Besitzes einer Fahrerlaubnis zur Durchführung des Beschäftigungsverhältnisses i.S.v. § 32 Abs. 1 Satz 1 BDSG erforderlich. Fraglich ist, ob nun auch die Führerscheinüberprüfungen bei Mitarbeitern, die Fahrzeuge i.R.e. Firmenwagenregelung als Bonus oder zur Repräsentanz erhalten, als durch § 32 Abs. 1 Satz 1 BDSG legitimiert angesehen werden können. Diese Beschäftigungsverhältnisse könnten – theoretisch – auch ohne Nutzung eines Firmenwagens durchgeführt werden.

Allerdings sollte der Begriff der Erforderlichkeit an dieser Stelle nicht restriktiv ausgelegt werden. Es entspricht den üblichen Gegebenheiten der heutigen Arbeitswelt, dass Dienstwagenregelungen bestehen, die vorsehen, dass die Überlassung eines Fahrzeugs ein Bestandteil des Vergütungspakets ist. In diesem Sinne verstanden ist die Führerscheinüberprüfung bei sämtlichen Mitarbeitern, denen ein Fahrzeug zur Nutzung überlassen wird, erforderlich i.S.v. § 32 Abs. 1 Satz 1 BDSG. Aber selbst wenn man diese Auffassung nicht teilt, ist die Datenverarbeitung in diesen Fällen rechtmäßig, da sie jedenfalls durch die gegenüber § 32 BDSG subsidiäre Norm des § 28 Abs. 1 Satz 1 Nr. 2 BDSG legitimiert ist. Die Verbindung einer Vertragsbeziehung mit einem Arbeitsverhältnis ist dabei unschädlich.[6] Die Überprüfung der Führerscheine ist jedenfalls zu Beginn der Firmenwagennutzung und anschließend in einem jährlichen Turnus zulässig.[7] Allerdings sind hierbei auch die Betriebsgröße und die Anzahl der zur Verfügung gestellten Fahrzeuge zu berücksichtigen.[8]

Zu bedenken ist auch, dass bei der Ablage von Führerscheinkopien in die Personalakte die allgemeinen datenschutzrechtlichen Anforderungen an die Führung von Personalakten (Einsichtsrechte etc.) zu beachten sind. Schließlich ist zwischen dem Unternehmen und einem etwaig genutzten Dienstleister, der die Überprüfung der Führerscheine übernimmt, eine Auftragsdatenverarbeitung gegeben, sodass auch in diesem Verhältnis die §§ 11, 9 BDSG i.V.m. Anlage zu § 9 Satz 1 zu beachten sind.

---

1 Mitt. des *Hamburgischen Datenschutzbeauftragten*, abrufbar unter: http://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-gps-ortung-von-mietwagen.html; s. hierzu: Unzulässige GPS-Ortung von Mietwagen, ZD-Aktuell 2012, 20; zur GPS-Ortung im Arbeitsverhältnis vgl. *Gola/Wronka*, Hdb. zum Arbeitnehmerdatenschutz, 5. Aufl. 2010, Rdnr. 902.

2 *Petri*, in: Simitis (Hrsg.), BDSG, 7. Aufl. 2011, § 11 Rdnr. 22; *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 11 Rdnr. 14.

3 *Gabel*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 11 Rdnr. 15.

4 BGHSt 6, 362; *OLG Frankfurt/M.* NJW 1965, 2312; *OLG Köln* VersR 1969, 741.

5 Vgl. hierzu *Gola/Schomerus* (Hrsg.), BDSG, 11. Aufl. 2012, § 4a Rdnr. 19 ff.; a.A. *Riesenhuber*, RdA 2011, 257, 261; vgl. zum Ganzen *Thüsing*, Arbeitnehmerdatenschutz und Compliance, 2010, Rdnr. 117 ff.

6 *Gola/Schomerus* (o. Fußn. 5), § 32 Rdnr. 31.

7 *Mielchen/Meyer*, DAR 2008, 5, 7.

8 *König*, SVR 2008, 121, 125.

3. Mitbestimmungspflichtigkeit gem. § 87 Abs. 1 Nr. 6 BetrVG

Mit den Elementen der Auftragsdatenverarbeitung und der Datenverarbeitung im Beschäftigungsverhältnis sind die datenschutzrechtlichen Belange des Fleetmanagements jedoch noch nicht gelöst. Fraglich ist vielmehr, ob die Einrichtung eines solchen Systems mitbestimmungsbedürftig ist. Gem. § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, mitzubestimmen. Im Rahmen des Fleetmanagements wird üblicherweise insbesondere die Schadensabwicklung durch den Anbieter übernommen. Diese Daten wiederum werden dann IT-gestützt an den Auftraggeber weitergeleitet. Dadurch kann ein Bild dessen entstehen, wie der Arbeitnehmer mit dem ihm überlassenen Fahrzeug umgeht und wie er es einsetzt.

Doch kann hierin bereits eine Überwachung des Verhaltens oder der Leistung des Arbeitnehmers gesehen werden? Die Mitbestimmungspflichtigkeit setzt zunächst das Vorliegen einer technischen Einrichtung voraus. Dabei wird der Begriff der technischen Einrichtung weit gefasst und beinhaltet alle optischen, akustischen, mechanischen und elektronischen Geräte.[9] Der Datenaustausch zwischen Auftraggeber und -nehmer findet regelmäßig softwaregestützt über automatisierte Systeme statt. Nach dem erwähnten weiten Verständnis einer technischen Einrichtung kann auch die Einführung und Anwendung einer Software mitbestimmungspflichtig sein.[10] Diese technische Einrichtung müsste nun dazu bestimmt sein, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Unter Überwachung wird dabei zunächst ein Vorgang verstanden, durch den Informationen über das Verhalten oder die Leistung der Arbeitnehmer erhoben und in aller Regel aufgezeichnet werden, um sie so der menschlichen Wahrnehmung zugänglich zu machen.[11]

Der Begriff der Überwachung wird darüber hinaus auf die bloße technische Auswertung von manuell, also nicht durch die technische Einrichtung selbst erhobenen Informationen erweitert.[12] Auch hier kann nach dem herrschenden weiten Verständnis des Begriffs der Überwachung durchaus von einer Überwachung der Arbeitnehmer durch die Datenweitergabe vom Flottenmanagementbetreiber zum Auftraggeber ausgegangen werden, da Informationen über das Verhalten der Arbeitnehmer, d.h. ihren Umgang mit den ihnen überlassenen Fahrzeugen zugänglich gemacht werden. Gegenstand der Überwachung muss das Verhalten oder die Leistung der Arbeitnehmer sein. Unter Verhalten versteht man dabei ein individuell steuerbares Tun.[13] Unter Leistung wird die vom Arbeitnehmer in Erfüllung seiner vertraglichen Pflicht geleistete Arbeit verstanden.[14] Bei der Nutzung des Fahrzeugs fallen naturgemäß Daten, wie die zurückgelegten Kilometer, Schadensdaten und Verkehrsordnungswidrigkeiten, an. Ist das Fahrzeug zudem mit Location Based Services oder einem GPS-Sender ausgestattet, fallen zusätzlich noch Standortdaten an, die zur Bildung eines Bewegungsprofils geeignet sind.[15] Daher können diese Daten durchaus Rückschlüsse jedenfalls auf das Verhalten der Arbeitnehmer, die einen Firmenwagen nutzen, ermöglichen. Dies ist allerdings bei der alleinigen Ausrüstung eines Firmenwagens mit einem Navigationssystem abzulehnen.[16] Fraglich ist jedoch, ob das Fleetmanagementsystem zur Überwachung der Arbeitnehmer bestimmt ist. Schließlich steht bei der Einrichtung eines Flottenmanagements nicht die Überwachung der Mitarbeiter, sondern deren Zugang zu Firmenwagen im Vordergrund.

Allerdings wird das Kriterium der Bestimmtheit durch die Rechtsprechung sehr extensiv ausgelegt. So wird eine Bestimmung zur Überwachung bereits angenommen, wenn die technische Einrichtung objektiv geeignet ist, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen.[17] Nach diesem weiten Verständnis, welches i.R.d. richterlichen Rechtsfortbildung die Wortlautgrenze überdehnt, könnte die Übermittlung von Arbeitnehmerdaten im Fleetmanagementsystem durchaus i.S.v. § 87 Abs. 1 Nr. 6 BetrVG zur Überwachung des Verhaltens der Arbeitnehmer geeignet sein. So ist regelmäßig auch die Einführung einer Software, die leistungs- und verhaltensrelevante Daten aufzeichnet und speichert, mitbestimmungspflichtig.[18] Allerdings ist die Einrichtung eines Fleetmanagementsystems mit dieser Konstellation nicht vergleichbar und weist einen entscheidenden Unterschied auf: Entgegen der Einführung einer technischen Einrichtung, die dazu geeignet ist, die Mitarbeiter insgesamt zu überwachen, betrifft die Datenverarbeitung innerhalb des Fleetmanagementsystems nur das Arbeitsverhältnis des jeweils zur Nutzung eines Firmenwagens berechtigten Mitarbeiters, da Fahrzeuge nicht pauschal an sämtliche Mitarbeiter eines Unternehmens vergeben werden. Die Mitbestimmungsrechte des Betriebsrats setzen jedoch voraus, dass es sich bei den in Rede stehenden Maßnahmen um kollektive Maßnahmen handelt. Maßnahmen, die auf einzelne Arbeitsverhältnisse abzielen, sind demgegenüber mitbestimmungsfrei.[19] Demnach sind auch die Maßnahmen innerhalb des Fleetmanagementsystems mitbestimmungsfrei. Zusätzlich kann es sich jedoch aus Gründen der Rechtssicherheit im Einzelfall empfehlen, die Arbeitnehmerdaten zu anonymisieren.[20]

III. Fazit

Die beim Fleetmanagement zur Datenübermittlung genutzten Systeme sind nicht mitbestimmungspflichtig, da sie keine kollektiven Maßnahmen darstellen, sondern einzig das Arbeitsverhältnis der jeweils zur Nutzung eines Firmenwagens berechtigten Mitarbeiters betreffen. Aus Sicht der Unternehmen ist zudem darauf zu achten, dass mit sämtlichen am System beteiligten Dienstleistern, d.h. mit dem Fuhrparkanbieter selbst sowie mit etwaig genutzten weiteren Dienstleitern, Verträge zur Auftragsdatenverarbeitung abgeschlossen werden. Werden diese Voraussetzungen beachtet, steht der Einrichtung eines datenschutzrechtskonformen Fleetmanagementsystems nichts im Wege.

Markus Schröder, LL.M. (Informationsrecht)
ist Rechtsanwalt und Datenschutzbeauftragter (TÜV) bei Kinast & Partner Rechtsanwälte, Externe Datenschutzbeauftragte in Köln, sowie Dozent für Datenschutzrecht an der Düsseldorf Law School.

9 *Klebe*, in: Däubler/Kittner/Klebe, BetrVG, 13. Aufl. 2012, § 87 BetrVG Rdnr. 137.
10 *Worzalla*, in: Hess/Schlochauer/Worzalla/Glock/Nicolai/Rose, BetrVG, 8. Aufl. 2011, § 87 Rdnr. 348.
11 *BAG* v. 6.12.1983, AP Nr. 7 zu § 87 BetrVG 1972 Überwachung.
12 *BAG* v. 14.9.1984, 23.4.1985, 11.3.1986, AP Nr. 9, 12, 14 zu § 87 BetrVG 1972 Überwachung.
13 *BAG* v. 11.3.1986, AP Nr. 14 zu § 87 BetrVG 1972 Überwachung; *Müllner*, DB 1984, 1677; *Matthes*, RDV 1985, 16, 21.
14 *BAG* v. 23.4.1985, 18.2.1986, AP Nr. 12, 13 zu § 87 BetrVG 1972 Überwachung.
15 Zur datenschutzrechtlichen Zulässigkeit von Location Based Services vgl. *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 5. Aufl. 2012, S. 186; *Gola/Wronka* (o. Fußn. 1), Rdnr. 904 ff.; *Steidle*, MMR 2009, 167; *Roßnagel*, NZV 2006, 281; *Article 29 Working Party*, Working document on data protection and privacy implications in eCall initiative, WP 125.
16 *Moll/Roebers*, DB 2010, 2672.
17 St. Rspr. seit *BAG* v. 9.9.1975, AP BetrVG 1972 § 87 Überwachung Nr. 2.
18 *Wedde*, DuD 2007, 752, 755; *Bender*, in: Wlotzke/Preis/Kreft, BetrVG, 4. Aufl. 2009, § 87 Rdnr. 127; *Kania*, in: Erfurter Komm. zum Arbeitsrecht, 12. Aufl. 2012, § 87 BetrVG Rdnr. 62; zu weiteren Beispielen vgl. *Werner*, in: Rolfs/Giesen/Kreikebohm/Udsching (Hrsg.), BeckOK-Arbeitsrecht, § 87 BetrVG Rdnr. 95.
19 *Wybitul*, Hdb. Datenschutz im Unternehmen, 2011, Rdnr. 219; *Thüsing* (o. Fußn. 5), Rdnr. 535.
20 *Gebhardt/Unmuß*, NZA 1995, 103, 107 ff.

Datenschutz im Krankenhaus

Rezension von Barbara Stöferle

Das bewährte Standardwerk für Datenschutz in Krankenhäusern wurde 2012 umfassend überarbeitet und ergänzt. Gleich geblieben ist der gut strukturierte Aufbau in Gesetzliche Grundlagen - Ärztliche Schweigepflicht – Verwendung von Patientendaten innerhalb des Krankenhauses – Übermittlung von Patientendaten an Dritte. In eigenen Kapiteln werden Sozialversicherungsträger/MDK sowie Unfallversicherungsträger behandelt. Ergänzt wird das Werk noch durch kurze Kapitel zum Datenschutzbeauftragten, Formen der Datenübermittlung wie sowie der Ausführung von seltenen, aber wichtigen Einzelfällen.

Das Werk eignet sich hervorragend als Nachschlagewerk für Fälle im Alltag eines Datenschutzbeauftragten. Sowohl über das Inhalts- als auch das Stichwortverzeichnis findet man schnell den gesuchten oder einen ähnlich gelagerten Anwendungsfall. Die Autoren belassen es nicht nur bei einer kurzen Antwort, sondern diskutieren die Fälle und verweisen dabei auf die relevanten Rechtsnormen oder einschlägigen Urteile. Dadurch erhält der Leser eine fundierte Hilfestellung.

Grundlegend überarbeitet wurde das Kapitel Dokumentation und Archivierung. Der Leser findet hier Hinweise, wie er seine gewünschte Archivierungslösung rechtskonform umsetzen kann. In diesem Kapitel wird auch auf die Orientierungshilfe KIS verwiesen, die gerne auch in den anderen Kapiteln mehr Einklang finden darf. Neu hinzugekommen sind Ausführungen zur Datenübermittlung gemäß § 294 a SGB V, Bundeskinderschutz- sowie Patientenrechtegesetz.

Das Werk ist – zur Recht – zu einem unverzichtbaren Standard- und Nachschlagewerk zu Datenschutzfragen im Krankenhaus geworden.

Info: Hauser/Haag: Datenschutz im Krankenhaus, Deutsche Krankenhaus Verlagsgesellschaft mbH, 4. Auflage 2012, 372 S., 45,- €

Datenschutz im Gesundheitswesen

Rezension von Barbara Stöferle

Das Loseblattwerk erschien 2012 und ist mit dem Untertitel „Grundlagenwissen - Praxislösungen – Entscheidungshilfen“ versehen. Diesem wird es voll gerecht. Das Werk ist in die drei Teile „Grundlagen“, „Bereichsspezifischer Datenschutz“ und „IT-Knowhow“ gegliedert. In den „Grundlagen“ wird sehr gut die Anwendung der besonderen rechtlichen Grundlagen beim allgemeinen Datenschutzrecht, Sozialgeheimnis, ärztliche Schweigepflicht bis hin zu den Spezialregelungen der Kirchen bzw. Länder beschrieben. Anschaulich - mit Beispielen aus dem Alltag - und einprägsam werden die Besonderheiten bei Betroffenenrechte, Einwilligung oder Auftragsdatenverarbeitung dargestellt. Die Aufgaben des Datenschutzbeauftragten, Aufbau eines Datenschutzmanagements und IT-Organisation werden in weiteren Kapiteln des Teils „Grundlagen“ beschrieben. Auch hier sind im Werk anschauliche Zusammenfassungen und Beispiele aus dem Bereich Patientendaten enthalten.

Der zweite Teil umfasst den bereichsspezifischen Datenschutz wie „Krankenhaus“, „GKV“ und „Arztpraxis“. Weitere Kapitel zu „Rehabilitation/Teilhabe“, „Pflege“ und „Beschäftigte“ sind für spätere Ergänzungen schon vorgemerkt. In diesen Kapiteln ist ein schneller Einstieg in praktische Alltagsfragen möglich. Allerdings sollte sich der Leser mit den „Grundlagen“ vertraut machen, um ein fundiertes theoretisches Wissen für die praktische Anwendung zu erhalten. Im Kapitel „Krankenhaus“ werden beispielsweise die datenschutzrelevanten Prozesse aus Sicht eines Patienten im Alltag erläutert. Themen wie interne Datenübermittlungen, Auftragsdatenverarbeitung oder Forschung könnten in den Ergänzungslieferungen vertieft werden. Beim Datenschutz in der GKV gibt es sehr viele konkrete gesetzliche Vorgaben, von denen man beim Einstieg leicht „erschlagen“ wird. Anhand von zahlreichen Fallbeispielen mit gleichzeitiger Darstellung der Gesetzesstellen und einschlägigen Urteilen erreicht der Autor jedoch, dass die gesetzlichen Bestimmungen anschaulich und im Alltag handhabbar bleiben. Beim Datenschutz in einer Arztpraxis werden ebenfalls die komplizierten Regelungen durch Beispiele erläutert. Auch wenn evtl. der eigene spezielle Anwendungsfall nicht erwähnt wird, so wird man sicherlich fündig, wie der Fall anzugehen ist.

Wie bringe ich als Mediziner (und Nicht-IT-Fachmann) der EDV bei, sich ebenfalls an Datenschutz und Schweigepflicht zu halten? Sicherlich kann auf ca. 140 Seiten des dritten Teils keine umfassende IT-Sicherheitsausbildung erfolgen. Dies ist auch nicht die Intention des Werkes. Der Autor erklärt – auch für nicht IT-Fachleute – verständlich die wichtigsten Grundbegrifft, Funktionsweisen und Zusammenhänge, so dass Risiken beim Einsatz von EDV-Geräten und Software besser beurteilt werden können. Stets auf die wichtigsten sicherheitsrelevanten Aspekte beschränkt, werden z.B. die verschiedenen Windows-Systeme mit ihren Vor- und Nachteilen und Sicherheitseinstellungen erläutert.

Info: Buchner (Hrsg.): Datenschutz im Gesundheitswesen, Remagen (AOK-Verlag) 2012, ca. 650 S., 169,- €

Betrieblicher Datenschutz – Schritt für Schritt zum erfolgreichen Datenschutzbeauftragten

Rezension von Udo Wenzel

Der betriebliche Datenschutz hat sich, spätestens seit der Novellierung des BDSG im Jahr 2001 und einhergehend mit den technischen Entwicklungen des letzten Jahrzehnts, kontinuierlich zu einem der wichtigsten Bausteine betrieblicher Compliance unterschiedlichster Branchen entwickelt. Und immer wieder stehen die Entscheider in den Unternehmen sowie deren zukünftige Datenschutzbeauftragte vor der Frage, welche Aufgaben mit dem betrieblichen Datenschutz auf sie zukommen und wie diese Aufgaben gelöst werden können. Deshalb ist es gut, dass nun von Dr. Grit Reimann das praxisorientierte Buch „Betrieblicher Datenschutz – Schritt für Schritt zum erfolgreichen Datenschutzbeauftragten“ erschienen ist. Es tritt mit dem Anspruch an, jedermann die Grundlagen des betrieblichen Datenschutzes fundiert, aber ohne technischen Hintergrund zu vermitteln. Dabei gelingt der Autorin mit ihrem Buch was nicht immer glückt: betrieblichen Datenschutz begreiflich zu machen.

Auf insgesamt 110 Seiten und in 12 Kapiteln behandelt es die Themen des betrieblichen Datenschutzes sehr kurz und prägnant. Im Vordergrund steht nicht das Detailwissen, sondern der Wille, den Lesern aus unterschiedlichen Branchen einen klaren und strukturierten Überblick über das Fachgebiet zu geben. Die verschiedenen Bereiche des Datenschutzes wie beispielsweise der Datenschutzbeauftragte, die technisch-organisatorischen Maßnahmen zum Datenschutz, betriebliche Regelungen, Datenschutzaudit, Beschäftigtendatenschutz oder Datenverarbeitung im Auftrag sind nur einige der im Buch behandelten Themen, die übersichtlich dargestellt und in einer verständlichen Sprache vermittelt werden. Zu fast jedem Bereich gibt es im Buch Vorlagen, Mustertexte oder auch ergänzende Materialien aus der Mediathek des Beuth Verlages.

Insgesamt dienen die einzelnen Themen, Vorlagen und Materialien eher als Leitfaden und können beziehungsweise müssen noch individuell durch weitere Lektüre ergänzt oder an die eigenen Anforderungen angepasst werden. Das ist jedoch kein Nachteil, denn schließlich erleichtern die zahlreichen Beispiele nicht nur das Verständnis, sondern regen auch zum Weiterlesen an. Leider sucht der interessierte Leser vergeblich nach Hinweisen, die es ihm erlauben würden, weiterführende aktuelle Informationen zu finden. Um nur ein Beispiel zu nennen: Vermisst werden solche Hinweise im Kapitel „Der Datenschutzbeauftragte“. Der korrekten Darstellung, dass die Aufgaben sowie die Aus- und Weiterbildung des Datenschutzbeauftragten im BDSG nicht klar geregelt werden, könnte ein Hinweis auf den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. sowie dessen berufliches Leitbild des Datenschutzbeauftragten, und auf andere Institutionen des Datenschutzes wie GDD oder UDIS folgen. Den Leser würde es freuen.

In diesem Sinne ersetzt dieses Buch auch keine Ausbildung zum Datenschutzbeauftragten und ist dafür auch nicht gedacht. Als schneller Einstieg und als Nachschlagewerk für angehende Datenschutzbeauftragte oder auch praxiserprobte Datenschützer, die sich mal wieder neue Ideen holen wollen, ist dieses Buch bestens geeignet. Führungskräfte aus Unternehmen aller Branchen erhalten mit diesem Buch alle Informationen, um sich ein Bild über die Mindestanforderungen des betrieblichen Datenschutzes machen zu können, und um eine Entscheidung für die Bestellung eines betrieblichen Datenschutzbeauftragten treffen zu können. Neben der gebundenen Version ist das Buch auch alternativ oder zusätzlich als E-Book (pdf) erhältlich.

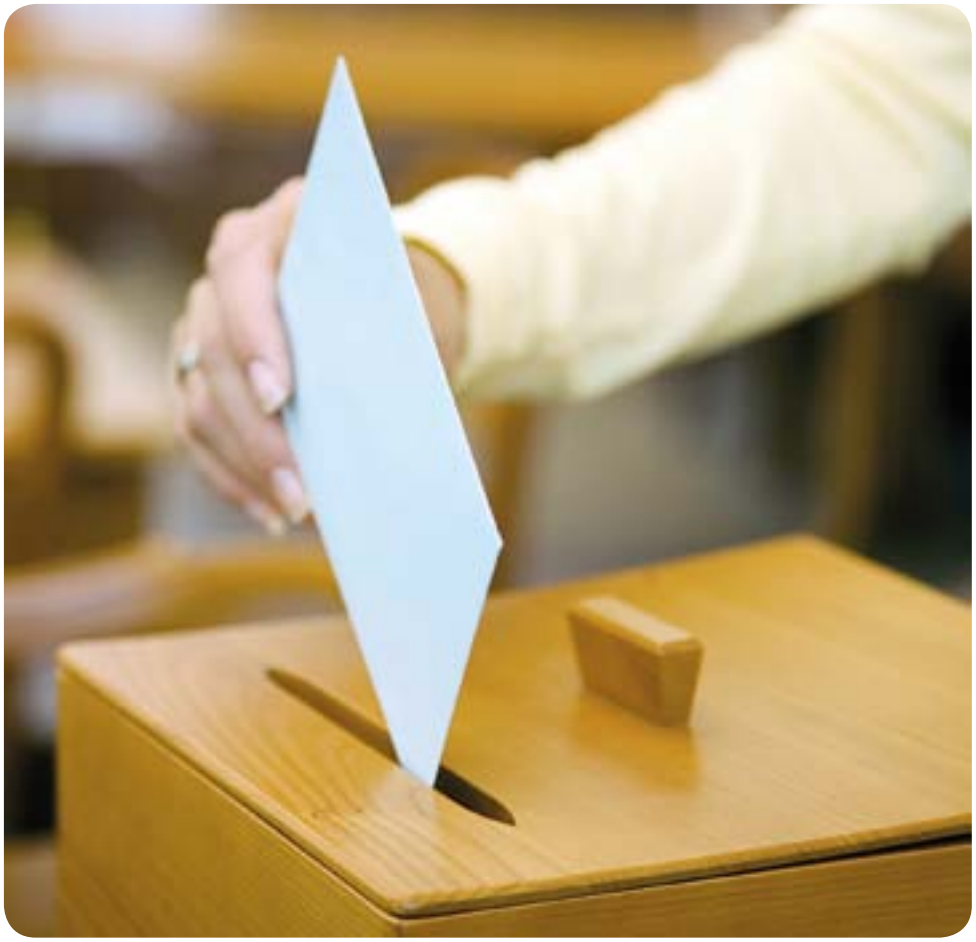
Info: Betrieblicher Datenschutz – Schritt für Schritt zum erfolgreichen Datenschutzbeauftragten, Dr. Grit Reimann, Beuth Verlag, Ausgabedatum 2013-02, ISBN 978-3-410-22760-1 56,- €

Wahlwerbung vermeiden

Widerspruchsrecht gegen Melderegisterauskünfte

Im Vorfeld der Bundestagswahl am 22. September 2013 weist der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Reinhard Dankert, darauf hin, dass die Wahlberechtigten ein Widerspruchsrecht gegen Melderegisterauskünfte zum Zwecke der Wahlwerbung haben.

Die Meldeämter dürfen Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit der Bundestagswahl aus dem Melderegister die Vor- und Familiennamen, Doktorgrade und Anschriften von Wahlberechtigten mitteilen, sofern die Betroffenen von ihrem Widerspruchsrecht keinen Gebrauch gemacht haben. Diese Melderegisterauskünfte können in den sechs der Wahl oder Stimmabgabe vorangehenden Monaten erteilt werden. „Nach wie vor ist dieses Widerspruchsrecht nur wenig bekannt. Wer nicht damit einverstanden ist, dass seine Daten für diesen Zweck von der Meldebehörde übermittelt werden, und lieber selbst darüber entscheiden möchte, bei welchen Parteien oder Kandidaten er sich informiert, kann von seinem gesetzlichen Widerspruchsrecht gegenüber der für ihn zuständigen Meldebehörde Gebrauch machen“, erklärt Reinhard Dankert. „Der Widerspruch ist kostenfrei und muss nicht begründet werden. Außerdem sollte man sich möglichst frühzeitig an das Meldeamt wenden. Ein einmal eingelegter Widerspruch gilt auch für künftige Wahlen. Es ist jedoch nicht möglich, den Widerspruch auf eine bestimmte politische Partei zu beschränken“, erklärt er weiter. Die Meldebehörden halten entsprechende Vordrucke bereit. Ein Mustertext findet sich unter der Adresse www.lfd.m-v.de.



Bevor der Wähler sein Kreuzchen macht, hat er unter Umständen schon verschiedene Versuche von Wahlwerbung der Parteien hinter sich. Dieser kann er jedoch widersprechen.

Das Seminarangebot des BvD auf einen Blick

Übersicht über die wichtigsten Termine des BvD bis zum Sommer

Mit seinem Seminarangebot bietet der BvD wichtige Fortbildungen für Datenschutzbeauftragte an. Die Teilnahmegebühr für eine eintägige Fortbildung beträgt 295,00 Euro (inkl. Verpflegung und Fortbildungsunterlagen). Jeder Teilnehmer erhält eine Teilnahmebescheinigung. Anmeldungen sind direkt über die BvD-Website https://www.bvdnet.de möglich.

Sonderseminar - Einführung in das Wettbewerbsrecht und Werberecht für bDSB (Referent: Dr. Schulze zur Wiesche, Datum: 24.04.2013, Ort: Berlin - NH Hotel Berlin Mitte)
Werbealltag. Auf manche Fragen gibt es eine datenschutz- und eine wettbewerbsrechtliche Antwort. Kenntnisse des Wettbewerbsrechts stellen für den Datenschutzrechtler einen echten Mehrwert dar. Dargestellt werden in diesem Seminar die strukturellen Grundzüge des Wettbewerbsrechts (UWG). Einen besonderen Schwerpunkt bilden die besonders „datenschutznahen" Bereiche des UWG, namentlich Direktmarketing und der Bereich „Rechtsbruch".

Sonderseminar - Facebook für Datenschutzbeauftragte (Referent: Christoph Heyn, Stefan Bachmann, Datum: 24.04.2013, Ort: Berlin - NH Hotel Berlin Mitte)
In diesem Seminar erfahren Sie das Wichtigste zum Umgang mit Facebook. Derzeit kommt wohl kein DSB um das Thema herum. Auch nach diesem Seminar werden Sie Facebook als Datenschutzbeauftragter nicht lieben, aber Sie wissen, worauf Sie achten und wo Sie Kunden und Mitarbeiter sensibilisieren müssen.

Seminar - Beschäftigtendatenschutz (Referent: Dr. Christian Bausewein, Datum: 07.05.2013, Ort: Frankfurt - NH Hotel Frankfurt Niederrad)
Ihnen werden für die Praxis die rechtlichen Grundlagen für den Umgang mit Beschäftigtendaten anschaulich vermittelt. Dr. Bausewein geht darauf ein, welche Besonderheiten beim Beschäftigtendatenschutz – Einwilligung und Betriebsvereinbarung betreffend – zu beachten sind. Ferner erhalten Sie neben relevanten Fragestellungen des Datenschutzes im Beschäftigungsverhältnis eine Überblick über die jüngste Rechtsprechung zum Beschäftigtendatenschutz.

Praxisseminar - Haftung des Datenschutzbeauftragten - als udis-Refresher anerkannt (Referent: Prof. Dr. Peter Wedde, Datum: 16.05.2013, Ort: Frankfurt - NH Hotel Frankfurt City)
Welche Haftungsrisiken bestehen für den Datenschutzbeauftragten und was kann er vorbeugend zur Minimierung dieser Risiken tun? Welche Beratungsqualität darf der Arbeitgeber oder Kunde verlangen und wie sind die gesetzlichen Regelungen? Praktische Fälle werden diskutiert, auf Fragestellungen eingegangen und Handlungsempfehlungen den Teilnehmern mit auf den Weg gegeben.

Praxisworkshop - Jura für Datenschutzbeauftragte - als udis-Refresher anerkannt (Referent: Dr. Jens Eckhardt, Datum: 17.05.2013, Ort: Düsseldorf - park inn Düsseldorf Süd)
Die Sprache der Juristen und die Wortwahl in den Gesetzestexten ist oft alles andere als klar verständlich oder gar logisch. Gerade die BDSG-Novelle II (z. B. § 28 Abs. 3 BDSG n. F. oder § 42a BDSG) zeigt, dass das Verständnis von Gesetzen für Nichtjuristen nicht immer leicht ist.Dieses Seminar soll Datenschutzbeauftragte mit entsprechender Vorbildung helfen, Gesetzestexte richtig zu lesen und richtig zu interpretieren. In diesem Workshop haben Sie die Möglichkeit, neben der Theorie in kleinen Gruppen die richtige Anwendung der Gesetze und der Rechtsfolgen zu erarbeiten und anzuwenden.

Seminar - Bring Your Own Device (BYOD) (Referent: Dr. Flemming Moos, Datum: 28.05.2013, Ort: Hamburg - NH Hotel Hamburg-Altona)
„Bring Your Own Device" (BYOD) ist einer der großen Trends, der die Unternehmens-IT bestimmt und verunsichert. Der Einsatz privater IT-Endgeräte wirft verschiedenste Fragen zur IT-Sicherheit und zum Datenschutz auf, die unbedingt vor der Einführung geklärt sein sollten.

Weitere Informationen finden sich in Seminarflyern wieder, die im Internet unter https://www.bvdnet.de zu finden sind oder bei der BvD-Geschäftsstelle angefordert werden können.

Die Termine der RGs und AKs auf einen Blick

Die wichtigsten Daten der BvD-Gremien

Die Arbeitskreise und Regionalgruppen sind wichtige Gremien innerhalb des BvD. Detaillierte Informationen zu den Treffen und den Terminen gibt es im Internet. Anmeldungen sind direkt über die BvD-Website https://www.bvdnet.de möglich.

RG Baden Treffen Waldkirch
10.04.2013 16:00 Uhr - 19:00 Uhr

RG Mitte Treffen Steinbach/Ts
11.04.2013 17:30 Uhr - 21:00 Uhr

AK Sozial Treffen in Fulda
18.04.2013 09:30 Uhr - 17:00 Uhr

RG Ost Treffen Wittenberg
24.05.2013 17:00 Uhr - 20:00 Uhr

RG Nord Treffen
30.05.2013 14:00 Uhr - 19:00 Uhr

RG Süd Treffen Ulm
21.06.2013 10:00 Uhr - 17:00 Uhr

RG Bayern Treffen Unterschleißheim
28.06.2013 13:00 Uhr - 18:00 Uhr
Thema: IT-Sicherheitsrichtlinie & BYOD,
Referent: RA Harder, R. Eppli

RG Baden Treffen Emmendingen
03.07.2013 16:00 Uhr - 19:00 Uhr

RG Mitte Treffen Obertshausen
04.07.2013 17:30 Uhr - 21:00 Uhr

RG Ost Treffen Berlin
17.09.2013 17:00 Uhr - 20:00 Uhr

RG Nord Treffen
26.09.2013 14:00 Uhr - 19:00 Uhr

RG Baden Treffen (Ort noch unklar)
09.10.2013 16:00 Uhr - 19:00 Uhr

RG Süd Treffen Ulm
18.10.2013 10:00 Uhr - 17:00 Uhr

RG Bayern Treffen Unterschleißheim
25.10.2013 13:00 Uhr - 18:00 Uhr
Thema: EU-Datenschutzverordnung
+ Fragestunde, Referent: Thomas Kranig

RG Ost Treffen Dresden
13.12.2013 15:00 Uhr - 20:00 Uhr

7 gute Gründe für eine Mitgliedschaft im BvD

► Fort- und Weiterbildung

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hält ein vielfältiges Angebot bereit. Speziell auf die Bedürfnisse ausgerichtete und vom BvD organisierte Fortbildungsseminare runden das Angebot ab. Alle Angebote und verschiedene externe Schulungen werden für BvD-Mitglieder zu besonders günstigen Konditionen durchgeführt. Insbesondere für Firmenmitglieder bieten sich wirtschaftliche Möglichkeiten, ihre Datenschutzmitarbeiter fortzubilden.

► Erfahrungsaustausch unter Kollegen

Das jährliche Highlight bilden die BvD-Verbandstage mit angeschlossener Fachmesse sowie mit integrierten Seminaren und Workshops. Erweitert wird dies um Fachtagungen und Symposien. Ein Datenschützer muss sich ständig am aktuellen rechtlichen Rahmen, an neuen Trends und Marktentwicklungen orientieren. Der BvD bietet für den Erfahrungsaustausch die Teilnahme an Regionalgruppen an. Für die Ausarbeitung von Fachthemen stehen die Arbeitskreise und Ausschüsse zur Verfügung.

► BvD-News / Fachpublikationen

BvD-Mitglieder erhaten die Datenschutz-Fachzeitschrift BvD-News – und viele weitere Fachpublikationen zu vergünstigten Konditionen.

► Entwicklung und Trends

Jedes Mitglied erhält durch die Zusammenarbeit des BvD mit anderen Verbänden, Interessengruppen und Organisationen laufend Informationen über aktuelle Trends und Studien im Datenschutz.

► Übersicht für Unternehmen

Der BvD hält eine Übersicht der auf das Berufsbild verpflichteten externen Datenschutzbeauftragten vor, die bei Bedarf an Aufsichtsbehörden, IHKs und Unternehmen weitergegeben werden kann. Diese wird quartalsweise aktualisiert.

► Chancen im Datenschutz

Der BvD hilft Ihnen, Klarheit über Funktionen, Stellenwert und Chancen des Datenschutzes zu gewinnen. Durch den BvD erfolgt auch mit Hilfe von Lobbyarbeit in Gesellschaft und Politik die Positionierung des Datenschutzes in Deutschland und auf europäischer Ebene: Er informiert regelmäßig Entscheider aus Wirtschaft und Politik über das Berufsbild sowie die Leistungen des Datenschutzbeauftragten.

► Engagement für die Gesellschaft

Mitarbeit und Unterstützung von gesellschaftlich bedeutenden Projekten und Initiativen. Der BvD ist Träger des Preises: „365 Orte im Land der Ideen 2011“.

Jetzt informieren:
www.bvdnet.de

Deutschland Land der Ideen
Ausgewählter Ort 2011

BvD e.V.
Die Datenschützer

BvD-Datenschutztage 2013

Datenschutz – Gestalten statt Verwalten!

24. und 25. April 2013 in Berlin

Deutschland Land der Ideen
Ausgewählter Ort 2011

BvD e.V.
Die Datenschützer

- 2 Tage intensives Networking und anregender Gedankenaustausch mit fachkundigen Teilnehmern, Referenten und Vertretern von Aufsichtsbehörden
- Herausragende Keyspeaker, u.a. Bundesjustizministerin Sabine Leutheusser-Schnarrenberger
- Sonderseminare zur Fortbildung
- BvD-Mitgliederversammlung
- Fundierte Workshops zu aktuellen Herausforderungen im Datenschutz, u.a. zu den Themen EU-Datenschutz-Grundverordnung, Audit und Dokumentation, Datenschutzorganisation im Konzern, Social Media, Beschäftigtendatenschutz

Veranstaltungsort: NH Berlin Mitte, Leipzigerstr. 106-111, 10117 Berlin

Wir haben im Tagungshotel NH-Berlin Mitte ein Kontingent an Zimmern für Sie reserviert: EZ 120,00 Euro incl. Frühstück, DZ 141,00 Euro incl. Frühstück Bitte buchen Sie direkt beim **NH-Berlin Mitte,** Stichwort „BvD-2013"

Anreise mit dem Zug
Nehmen Sie vom Hauptbahnhof die S5 in Richtung Straußberg oder die S7 in Richtung Ahrensfelde und steigen Sie an der Haltestelle Friedrichstraße aus. Steigen Sie in die U-Bahn U6 in Richtung Alt Mariendorf um und fahren Sie bis zur Haltestelle Stadtmitte. Das Hotel liegt auf der rechten Seite in der Leipziger Straße. Gesamtzeit: 10 bis 15 Minuten

Mit NH Ecomeeting und der Deutschen Bahn umweltfreundlich zu den Verbandstagen: Buchen Sie Ihr DB-Zugticket im Rahmen der BvD-Veranstaltung im NH-Berline Mitte. Tickets zum Vorteilspreis ab 99 Euro hin und zurück unter Tel: 0 18 05 . 31 11 53 (14 Ct./Minute), Stichwort NH Hoteles.

Anreise mit dem Flugzeug
Von Tegel: Fahren Sie mit der Buslinie 128 bis zur U-Bahnstation Kurt-Schumacher-Platz. Steigen Sie in die U6 in Richtung Alt Mariendorf um. Fahren Sie bis zur Haltestelle Stadtmitte. Gesamtzeit: 25 Minuten.

Von Schönefeld: Nehmen Sie die S7 oder S14 in Richtung Hauptbahnhof. Steigen Sie an der Haltestelle Friedrichstraße aus und steigen Sie in die U-Bahnlinie U6 in Richtung Alt Mariendorf um. Steigen Sie an der Haltestelle Stadtmitte aus. Gesamtzeit: 40 Minuten

Termin vormerken: 24. und 25. April 2013!