ISSN 2194-1025

AUSGABE 2/2013

BvD-News

Das Fachmagazin für den Datenschutz

Das neue Datenschutzaudit von BvD und GDD | *Alle Infos ab Seite 7*

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

BvD-Datenschutzsymposium am 17.10. | Seite 6

Interview mit Jan Philipp Albrecht | ab Seite 18

Neues BvD-Angebot „Datenschutz live“ | ab Seite 54

Vorstellung BvD Blog | ab Seite 59

BvD e.V.

Die Datenschützer

Jetzt 2 Ausgaben gratis testen!

Datenschutz im Fokus.

Sichern Sie, was Ihnen wichtig ist.

Mit dem Datenschutz-Berater – seit über 30 Jahren der verlässliche Ratgeber für Datenschutzbeauftragte.

Testen Sie den Datenschutz-Berater und profitieren Sie von folgenden Vorteilen:

- **2 Hefte Datenschutz-Berater:** Sie erhalten 2 Ausgaben Datenschutz-Berater pünktlich auf Ihren Schreibtisch. Der Informationsdienst Datenschutz-Berater berichtet seit über 30 Jahren über aktuelle Entwicklungen in Datenschutz und Datensicherheit und hilft Ihnen sich in der Informationsflut von Gerichtsentscheidungen, Gesetzen und Empfehlungen zurechtzufinden.

- **2 Monate kostenloser Zugriff auf www.datenschutz-berater.de** mit aktuellen News, Gesetzestexten, Literaturhinweisen, Veranstaltungstipps und dem Zugang zum Online-Archiv aller Ausgaben seit 2000.

Jetzt 2 Ausgaben gratis testen! www.datenschutz-berater.de/gratis1

Editorial

Liebe Leser,

mit dieser BvD-News-Ausgabe wagen wir erstmals den Schritt hin zu einer im üblichen Rahmen mit Werbung durchsetzten Ausgabe. Damit die BvD-News für Sie als Leser weiter kostenlos bleibt, werden wir versuchen, die richtige Verteilung von Fach- und Werbebeiträgen zu finden. Informationen zu Werbepartnern und Unterstützern finden Sie im Impressum.

An dieser Stelle möchte ich mich insbesondere bei den vielen Autoren für deren aktive unentgeltliche Mitarbeit bedanken. Ihnen bieten wir mit den BvD-News auch ein Forum, um über Fachbeiträge mit den Mitgliedern in einen Diskurs zu treten.

Die BvD-Geschäftsstelle hat endlich Verstärkung erhalten. Frau Claudia Melcher ist seit dem 15. September als Leiterin der Geschäftsstelle mit an Bord. Weiteres dazu finden Sie wie gewohnt unter „Aus der Geschäftsstelle".

EU-DSGVO – Wie geht es weiter?

Die Frage haben wir in zahlreichen Gesprächen während des politischen Sommers unseren Gesprächspartnern in Brüssel aber auch im BMI und im BMJ gestellt. Wir sind durchweg auf gegenüber dem Datenschutzbeauftragten aufgeschlossene Gesprächspartner gestoßen. Die Sorge über die Entwicklung der Gespräche in Brüssel war allen anzumerken.

Obwohl in der Öffentlichkeit immer wieder davon die Rede ist, dass man das hohe deutsche Datenschutzniveau auf die EU übertragen wolle, kann davon keine Rede sein. Mehrere Mitgliedsstaaten haben längst signalisiert, dass ihnen das zu viel des Guten sei (siehe auch das Interview mit Herrn Albrecht).

Im Rat ist inzwischen Verhandlungsstand, dass der DSB nur noch freiwillig bestellt werden soll. In Kommission und Parlament wird nun Druck gemacht, vor den Parlamentswahlen im Mai 2014 zu einem Abschluss zu kommen, offenbar ohne die vielen Lücken und Probleme der Verordnung vorher zu klären (siehe dazu auch den Artikel von Frau Dr. Mester). Wir werden unsere Arbeit hier fortsetzen und weiter auf die Defizite der Verordnung hinweisen. Ohne die Bundesregierung wird hier aber keine Änderung zu erreichen sein.

„DS-BvD-GDD-01"

Ein kryptischer Name für eine kleine Sensation: Der BvD und die GDD haben in einer mehr als eineinhalbjährigen Zusammenarbeit den ersten unabhängigen Datenschutzstandard für Auftragsdatenverarbeiter/IT-Dienstleister entwickelt und diesen der Aufsichtsbehörde aus NRW, dem LDI, zur Bewertung vorgestellt. Die Ergebnisse sind überaus erfreulich. Herr Lepper hat den Standard als ersten geeigneten offenen Datenschutzstandard für Auftragsdatenverarbeiter gelobt. Wir werden den Standard natürlich allen interessierten Aufsichtsbehörden vorstellen, damit diese sich ein eigenes Bild dazu machen können.

Die Verbände wollten damit einerseits den Unternehmen die Möglichkeit bieten, sich in diesem Bereich neu aufzustellen und andererseits den Mitgliedern ermöglichen, als Auditor oder auch als interner DSB von dieser Verbesserung zu profitieren. Wir werden bei zahlreichen kommenden Veranstaltungen über dieses Thema informieren (siehe dazu die Artikel ab S.7).

Sie sehen schon – die Arbeit geht uns nicht aus. Ich wünsche Ihnen eine spannende Lektüre!

Ihr Thomas Spaeing
BvD-Vorstandsvorsitzender

Kommunikation kann so einfach sein.

Als externer Datenschutzbeauftragter oder als Beratungsunternehmen stehen Sie regelmäßig in Kontakt mit aktuellen und potenziellen Kunden. Wichtig ist zunächst der erste Kontakt – und später eine kontinuierliche Kommunikation zur Pflege der Kundenverbindungen. Dafür sollte Ihre Außendarstellung stimmen.

Damit Sie dabei nicht auf der Leitung stehen, bieten wir Ihnen eine umfassende Unterstützung an:

- Strategien und Materialien zur Kundenakquise
- Marketingideen und direkte Umsetzungen in der Kundenpflege
- Redaktionelles Marketing über Pressemitteilungen, Stellungnahmen und Advertorials
- Ein sicheres Auftreten auf allen Kanälen, angefangen von der Internetseite bis zu verschiedenen Social Media-Kanälen

Sprechen Sie uns an: Wir erstellen Ihnen gerne ein unverbindliches Konzept und unterbreiten Ihnen Gestaltungsvorschläge für Ihr Corporate Design mit Broschüren, digitalen Materialien und mehr.

Ihr schneller Kontakt:
Medienhaus Waltrop
Michael Braun
braun@medienhaus-waltrop.de
Tel: 02309 . 7847113

MEDIEN HAUS WALTROP

Inhaltsverzeichnis

- Editorial 3
- BvD-Symposium 2013 gibt Anregungen und Impulse 6
- BvD und GDD entwickeln Datenschutzaudit 7
- Neuer Datenschutzstandard ist Basis für Prüfsiegel 10
- Datenschutzkonforme Wege ins Web 2.0 12
- Datenschutz „Made in Germany?“ 14
- „Optimistisch, dass es bis April 2014 eine Einigung gibt“ 18
- Datenschutz-Prüfungsaktion des BayLDA im Jahr 2013 22
- „Transparenz, aber kein Zugriff für alle“ 24
- Die EU-DSGVO aus Sicht französischer Behörden 26
- Jugendschutz-Programme – für ein sicheres Surfen? 30
- Die Stiftung Datenschutz als Partner in Bildungsfragen 33
- Datenschutzprüfung bei Einsatz von Adobe Analytics 36
- Mindestanforderungen an das Berufsbild des Compliance-Officer 40
- BYOD – Bring Your Own „Disaster“ 44
- 3. privacyGUARD-Kundentag 48
- Die neue Dimension der Datensicherheit 50
- So entsteht die „BvD-News“: Von der Idee zum fertigen Heft 52
- „Datenschutz live“: Neue BvD-Reihe startet mit Rhenus 54
- Experten drängen auf ein hohes Datenschutzniveau 56
- Neue Möglichkeiten der Diskussion - der BvD-Blog 59
- Mitarbeiterbefragungen – datenschutzrechtliche Vorgaben und Grenzen 62
- Runder Tisch zur Datenträger-Archivierung 65
- AK Externe nimmt Datenschutz in Österreich in Augenschein 68
- EU-DSGVO: Was wären die Folgen der Umsetzung? 70
- Erweiterung der BvD-Geschäftsstelle 72
- Der BvD in Zahlen 72
- Nächste Seminare der udis 73
- Seminare und Treffpunkte für BvD-Mitglieder 74

Hinweis: Der Druck dieser Ausgabe wurde maßgeblich von der Firma Rhenus Office Systems gesponsert.

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, Thomas Floß, Claudia Melcher, Claudia Seilert, Michael Braun, Romina Suliani

Fotos: Fotolia, iStockphoto, Medienhaus Waltrop

Lektorat: Frank Spaeing

Produktion (Planung, Satz, Layout, Verlag): ISB-Verlag im Medienhaus Waltrop, Bahnhofstraße 141, 45731 Waltrop, www.medienhaus-waltrop.de

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

ISSN: 2194-1025

Erscheinungsweise: 3 x jährlich, ca. 2500 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.

BvD-Symposium 2013 gibt Anregungen und Impulse

Veranstaltung als Plattform zur Diskussion von Fragen zum Beruf des Datenschutzbeauftragten – Vorstellung des neuen Audits

Programmergänzung

Aus aktuellem Anlass hat der BvD das Programm des Datenschutzsymposiums ergänzt: Dr. Niels Lepperhoff und RA Thomas Müthlein stellen unter dem Titel „Datenschutzaudit zur Auftragsdatenverarbeitung" den neuen Standard „DS-BvD-GDD-01" in einem Vortrag vor (siehe auch Berichte auf den nächsten Seiten).

Melden Sie sich jetzt an unter https://www.bvdnet.de.

Auf dem BvD-Datenschutzsymposium am 17. Oktober in Frankfurt präsentiert der BvD erfahrene Datenschützer aus international agierenden Unternehmen, die in ihren Vorträgen aus ihrer Praxis berichten und Diskussionsanstöße zum Beruf des Datenschutzbeauftragten geben. Die Veranstaltung soll zum regen Austausch von Erfahrungen und Know-how dienen. BvD-Mitglieder können sich direkt in der Geschäftsstelle oder über die BvD-Webseite https://www.bvdnet.de anmelden.

Der zunehmend internationale Datenschutz und die Bedingungen, unter denen Datenschutzbeauftragte heute und in Zukunft arbeiten, werden bei den Vorträgen im Mittelpunkt stehen. „Die Anforderungen an die Tätigkeiten der Datenschutzbeauftragten aus internationaler Perspektive steigen stetig an. Gerade die Unterschiedlichkeit des Datenschutzverständnisses in verschiedenen Ländern, selbst innerhalb der Europäischen Union, ist eine große Herausforderung der Gegenwart und der näheren Zukunft", erklärt BvD-Vorstandsvorsitzender Thomas Spaeing. Der BvD habe deswegen erfahrene Datenschützer aus international agierenden Unternehmen eingeladen, die über die Grenzen Deutschlands hinweg bereits wichtige Erfahrungen in Datenschutzbelangen gemacht haben. „Diese grundlegenden Erfahrungen machen sie auf diesem Symposium den BvD-Mitgliedern zugänglich", führt Thomas Spaeing aus. Nach jedem Vortrag wird ausreichend Zeit für Nachfragen und Diskussionen sein.

Dr. Thilo Weichert, Landesdatenschutzbeauftragter in Schleswig-Holstein, wird über unterschiedliche Sichtweisen und Ansprüche im internationalen Datenschutz sprechen. Manfred Speck, Head of Privacy and Information Security bei der Nestlé Deutschland AG, referiert über den Nutzen des Datenschutzes im internationalen Konzern. Internationale Anforderungen an die Tätigkeit des Datenschutzbeauftragten sind Thema bei Susanne Eichhorn, Vice President Privacy Employees, Stakeholders bei der Deutsche Telekom AG. Stefan Mairose, Leiter Datenschutz Audit bei der DB Mobility Logistics AG, wird schließlich über Methoden und Werkzeuge für Datenschutz-Controlling sprechen.

Info: Das komplette Programm und die Möglichkeit zur Anmeldung finden Sie im Internet unter der Adresse https://www.bvdnet.de.

BvD und GDD entwickeln Datenschutzaudit

Auftragsdatenverarbeitung: Neuer Standard „DS-BvD-GDD-01“ wird von der Aufsichtsbehörde NRW befürwortet

Die beiden großen Datenschutzverände BvD und GDD haben den ersten unabhängigen Datenschutzstandard für Auftragsdatenverarbeiter und IT-Dienstleister vorgestellt. BvD und GDD schaffen damit die Grundlage für klare Datenschutzstandards bei der Datenverarbeitung im Auftrag. Der Standard „DS-BvD-GDD-01“ gilt für alle Branchen und Dienstleistungen. Er beschreibt insbesondere, welche Anforderungen ein Auftragnehmer erfüllen muss. Vorgestellt wurde der neue Standard in Köln.

Das Interesse war groß – größer als gedacht. Die Stühle im Mevissensaal der Fachhochschule Köln reichten nicht aus, um allen Zuhörern einen Sitzplatz zu geben. Über 70 Gäste wollten sich am 25. September in einem Symposium über das Gemeinschaftsprojekt von BvD und GDD informieren: den ersten offenen Datenschutzstandard für die Auftragsdatenverarbeitung mit qualifiziertem Datenschutzsiegel.

Vier Referenten, darunter BvD-Vorstandsvorsitzender Thomas Spaeing und Rechtsanwalt Thomas Müthlein, Vorstandsmitglied der GDD, stellten den neuen Datenschutzstandard „DS-BvD-GDD-01“ und das dazugehörige Siegel genauer vor. Auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Ulrich Lepper, war gekommen und bewertete das Konzept hinter dem neu entwickelten Standard und Datenschutzsiegel aus Sicht der für NRW zuständigen Datenschutzaufsichtsbehörde. Der Tenor: Mit dem Standard wird Unternehmen für die Auftragsdatenverarbeitung ein klar nachvollziehbarer und datenschutzrechtlich korrekter Rahmen gegeben. Außerdem wird durch das auf dem Standard fußende Siegel die Qualität der Auftragsdatenverarbeitung unter datenschutzrechtlichen Gesichtspunkten „sichtbar“. Es ist das erste Mal, dass ein Standard von einer Aufsichtsbehörde befürwortet wird.

Welchen Nutzen die Zertifizierung für Auftrags-

BvD-Vorstandsvorsitzender Thomas Spaeing stellte den neuen Standard „DS-BvD-GDD-01“ über 70 Interessierten in Köln vor.

Autorinnen

Romina Suliani
Verena Hülssiep (Fotos)
Medienhaus Waltrop

Thomas Spaeing und Rechtsanwalt Thomas Müthlein (links), Vorstandsmitglied der GDD, stellten sich gemeinsam mit Ulrich Lepper, Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, den Fragen der Teilnehmer.

datenverarbeiter hat, erklärte Thomas Spaeing in seinem Beitrag. Die Kontrollpflicht der Auftragsdatenverarbeitung nach §11 BDSG stellt Spaeing zufolge die Auftraggeber vor eine große Herausforderung. Sowohl Kostenaufwand als auch Umfang der Kontrolle seien kaum vorher abzuschätzen. „Dazu kommt, dass Auftraggeber damit häufig schlichtweg überfordert sind Dienstleister zu prüfen, denn viele sind gar nicht so genau im Thema, dass sie wüssten, was genau zu tun ist und nach welchen Standards genau geprüft werden soll", sagte Spaeing. Die Folge: Häufig werde die Prüfung übertrieben, es würden Dinge verlangt, die gar nicht notwendig seien. „Auf der anderen Seite sind die Dienstleister aus der Auftragsdatenverarbeitung häufig außer Stande, die Anforderungen zu erfüllen", erklärte der BvD-Vorstandsvorsitzende weiter. Dies gelte besonders für kleine und mittelständige Unternehmen. „Schon jetzt gibt es eine ganze Reihe von Gütesiegeln, die von den jeweiligen Anbietern selbst erfunden werden. Zu Grunde liegen Standards, die keiner kennt", gab Spaeing zu bedenken. Daher profitierten sowohl Auftraggeber als auch Auftragnehmer von einem einheitlichen, neutralen und transparenten Standard. „Und als Berufsverbände sind BvD und GDD in der Rolle, einen solchen neutralen Standard entwickeln zu müssen – und zu können, denn in ihnen trifft sich das gesammelte Datenschutz-Know-how." Die hohe Transparenz, die enorme Fachkunde und die daraus entstehende Wirtschaftlichkeit für Unternehmen sind laut Spaeing kurz und bündig zusammengefasst die wichtigsten Vorteile.

Dieser Meinung schloss sich auch Rechtsanwalt Thomas Müthlein in seinem Vortrag an. Er stellte den Datenschutzstandard „DS-BvD-GDD-01" genauer vor und erklärte sein grundsätzliches Konzept. Aus seiner eigenen Beratungspraxis kennt Müthlein die Fälle, in denen die Kontrolle der Auftragsdatenverarbeitung ohne Standard sowohl auf Seiten der Auftraggeber als auch Auftragnehmer zu erheblichen Unsicherheiten führt. „Daher ist es wichtig, Klarheit für beide Seiten zu schaffen, welche Herausforderungen an einen Auftragnehmer im Rahmen einer Auftragsdatenverarbeitung gestellt werden können", sagte Müthlein zusammenfassend. Auch ist ihm die Förderung des Datenschutzes in der Fläche ein wichtiges Anliegen. Und auch diesem Umstand werde mit einem einheitlichen Standard Rechnung getragen. Dass zusätzlich zu dem Datenschutzstandard auch noch ein zertifizierendes Siegel auf den Weg gebracht wurde, bezeichnete Müthlein als „Sahnehäubchen".

Die besondere Qualität dieses „Sahnehäubchens" erläuterte Dr. Niels Lepperhoff in seinem Vortrag. Er ist der Geschäftsführer der DSZ Datenschutz Zertifizierunggesellschaft mbH. GDD und BvD gründeten sie als zentrale Zertifizierungsstelle für die Durchführung der Standardüberprüfung, die Verwaltung und Vergabe der Datenschutzgütesiegel. Außerdem qualifiziert sie auch die Auditoren. „Datenschutz ist unsichtbar", sagte Lepperhoff. „Unser

Gütesiegel hilft dem Auftragnehmer nach außen zu zeigen, dass er den Standard erfüllt. Nicht durch eine Selbsterklärung – das glaubt keiner im Markt. Sondern auf Grundlage eines unabhängigen Prüfungsverfahrens. Deswegen gehen Standard und Gütesiegel Hand in Hand.“ Das Siegel soll für Auftragnehmer und -geber Vertrauen schaffen, es soll zeigen, dass ein Unternehmen nach einem offenen Standard geprüft wurde. Übrigens können die Prüfungsprotokolle jedes erfolgreich geprüften und zertifizierten Betriebes öffentlich eingesehen werden. So profitieren auch solche Unternehmen, die sich noch zertifizieren lassen möchten: Auf einen Blick erkennen sie Kriterien und Prüfungsverfahren.

Der von BvD und GDD entwickelte Standard war zudem der erste, den eine Aufsichtsbehörde geprüft hat. Ulrich Lepper, Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, begrüßte in seiner Bewertung das Konzept ausdrücklich: „Standards, die auch von der Aufsichtsbehörde befürwortet werden, leisten einen Beitrag zur Rechtssicherheit.“ Der Datenschutzstandard „DS-BvD-GDD-01“ zeichne sich besonders durch seine umfangreiche Ausarbeitung aus. „Das Modell mit seinem Rollenkonzept und das Zertifizierungsverfahren sind aus Sicht der Aufsichtsbehörde zu befürworten und eine Prüfung in der Praxis wert.“ Außerdem könne er sich gut vorstellen, das Modell auch im politischen Diskurs einzubringen, wenn es beispielsweise darum gehe, dass der Gesetzesgeber Regelungen zum Audit schaffen soll. „Ich bin von dem Modell, von der theoretischen Konzeption überzeugt“, sagte Lepper. Der Standard sei seiner Ansicht nach eine geeignete Grundlage für weitere Schritte, um einen offenen, unvoreingenommenen Dialog zu führen. „Ziel ist eine Lösung nicht nur auf Landes- sondern auf Bundesebene zu finden“, blickte Lepper in die Zukunft. „Jetzt müssen wir sehen, wie es sich in der Praxis bewährt.“ Er sei aber schon jetzt gerne bereit, für die Idee etwa bei der Datenschutzkonferenz und dem Düsseldorfer Kreis zu werben. „Ich bin überzeugt, dass die Erfahrungen, die wir hier mit dem Modell und im offenen Diskurs machen werden, Einfluss auf die Gesetzgebung haben werden.“

Im Plenum fand die Idee des Datenschutzstandards und des dazugehörigen Gütesiegels positive Resonanz. Frederick Richter, Vorstand der Stiftung Datenschutz, schätzte an dem Gemeinschaftsprojekt von BvD und GDD vor allem die Fachkompetenz, die dahinter steht: „Es ist ein sehr vielversprechender Ansatz, wenn sich eine solche fachliche Expertise zusammenschließt und so einen Standard auf den Weg bringt. Sehr begrüße ich, dass es ein offener Standard ist, der sich mit weitergehenden Vorhaben wie dem bundesweiten Datenschutzgütesiegel, den die Stiftung Datenschutz plant, verzahnen lässt. Das widerspricht sich meiner Ansicht nach überhaupt nicht.“ Die Ergebnisse und Erfahrungen aus der Anwendung des Datenschutzstandards für die Auftragsdatenverarbeitung kann man dann auch weitergehend nutzen, für den Aufbau eines allgemeinen Datenschutzstandards, ist sich Richter sicher.

Als bereits zugelassener Auditor der Deutschen Sachverständigen Gesellschaft (DESAG) kennt BvD-Vorstand Thomas Floß die Bedürfnisse des Kunden und findet den Datenschutzstandard und das Gütesiegel deshalb besonders lobenswert: „Für die Kunden ist ein Standard unglaublich wichtig, weil sie eine neutrale Person auf einen Prozess schauen lassen und dann ihren Auftraggebern zeigen können, dass sie von Extern für gut befunden wurden“ Da es bislang kein einheitliches Siegel gibt, das von einer Aufsichtsratbehörde befürwortet wurde, sei das Konzept von BvD und GDD sehr gut und wegweisend für künftige Entwicklungen.

Hinweis: Ab sofort kann sich jeder unter http://www.dsz-audit.de ausführlich über den Standard, über die Gütesiegelvergabe sowie die Ausbildung zum Auditor informieren.

Im Anschluss an die Vorstellung wurde der neue Standard kontrovers diskutiert.

Neuer Datenschutzstandard ist Basis für Prüfsiegel

Dr. Niels Lepperhoff über das neue Angebot von BvD und GDD

Ein gutes Datenschutzniveau in einem Unternehmen ist unsichtbar. Es lässt sich weder an Produkteigenschaften noch an Kennzahlen wie Umsatz oder Mitarbeiteranzahl festmachen. Der BvD e.V. und die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) haben deshalb ein Datenschutzsiegel basierend auf dem Datenschutzstandard „DS-BvD-GDD-01" speziell für die Auftragsdatenverarbeitung entwickelt. BvD-News-Redakteur Michael Braun sprach mit Dr. Niels Lepperhoff, dem Geschäftsführer der von BvD und GDD gegründeten DSZ Datenschutz Zertifizierungsgesellschaft mbH, über den neuen Standard, das neue Siegel und den Hintergrund des neuen BvD-Angebotes.

BvD-News: Herr Dr. Lepperhoff, BvD und GDD haben sich zusammengetan, um gemeinsam einen Standard zur Auftragsdatenverarbeitung zu entwickeln, der von Auditoren überprüft und der mit einem Prüfsiegel bestätigt wird. Wie läuft das Verfahren kurz zusammengefasst ab?

Dr. Niels Lepperhoff: Der Datenschutzstandard „DS-BvD-GDD-01" ist Grundlage zur Erteilung des von BvD und GDD entwickelten Datenschutzsiegels. Vergeben wird dieses Siegel von der DSZ Datenschutz Zertifizierungsgesellschaft mbH, einem gemeinsamen Unternehmen von BvD und GDD. Vor Erteilung des Siegels wird die Auftragsdatenverarbeitung von einem von der DSZ zertifizierten Auditor geprüft.

BvD-News: Welche Beweggründe für die Formulierung des Standards gab es?

Dr. Niels Lepperhoff: Das Angebot von BvD und GDD ist dazu da, um einen Mangel zu beheben, der sich aus § 11 BDSG (Auftragsdatenverarbeitung) ergibt. Er ist sehr unklar formuliert, es gibt viele Unsicherheiten, wie die Ausführungen des § 11 gemeint sind. Niemand weiß mit Sicherheit, was er tun muss, und das macht die Praxis enorm schwierig. Der neue Standard wurde von Datenschutz-Experten aus der Praxis heraus entwickelt. Der Standard ist offen und für jedermann einsehbar. Die Einhaltung dieses Standards wird durch die Vergabe eines Siegels bescheinigt. Die Konzeption aus öffentlich zugänglichem Standard sowie neutraler und transparenter Zertifizierung mit ausgewiesenen Datenschutzexperten überzeugt aus unserer Sicht.

BvD-News: Was genau ist denn an Unsicherheiten vorhanden?

Dr. Niels Lepperhoff: Der Gesetzgeber stellt zwar klar, dass vor Auftragsvergabe eine Überprüfung zur Auftragsdatenverarbeitung erfolgen muss – und dass es sie auch danach geben muss. Er spricht jedoch nur von einer regelmäßigen Kontrolle, ohne konkrete Zeiträume zu benennen. Unklar ist auch, in welcher Form kontrolliert werden soll.

BvD-News: Es gibt ja bereits Prüfsiegel und Zertifikate am Markt. Warum jetzt das Siegel von BvD und GDD?

Dr. Niels Lepperhoff: Die bisherigen Segel hatten Schwächen – sie waren intransparent und vor allem – sie hatten nicht die Unterstützung durch eine Aufsichtsbehörde.

BvD-News: Und das ist jetzt anders?

Dr. Niels Lepperhoff: Genau. Mit dem Standard DS-BvD-GDD-01 und dem damit verbundenen Siegel liegt erstmals eine Gesamtkonzeption aus Standard und Zertifizierungsablauf vor, die von einer Aufsichtsbehörde – in dem Fall durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) – befürwortet wird (siehe https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Wirtschaft/Inhalt/Modellvorhaben_Datenschutzsiegel/Modellvorhaben_Datenschutzsiegel.pdf).

Der neue Standard beschreibt zudem konkret und transparent, welche Pflichten Auftraggeber wie Auftragnehmer in der Auftragsdatenverarbeitung haben. Er berücksichtigt die Betriebswirklichkeit und funktioniert dabei vollkommen unabhängig: Jede Technik und jede standardisierte Leistung wird unterstützt. Der neue Datenschutzstandard ist zudem öffentlich verfügbar und einsehbar. Dazu kommt wie gesagt die Qualitätsaussage der Behörde.

BvD-News: Sie betonen die öffentliche Verfügbarkeit und die Transparenz. Können Sie diese Aspekte genauer ausführen?

Dr. Niels Lepperhoff: Das Siegel ist sozusagen zweifach neutral: Scharfe Regeln zur Interessensfreiheit geben zum einen vor, dass weder der Auditor noch Mitglieder des Zertifizierungsausschusses mit dem zu prüfenden Unternehmen wirtschaftlich verbunden sein dürfen. Das gilt für Vergangenheit und Zukunft: Es ist ihnen untersagt, in den folgenden 12 Monaten Aufträge des Unternehmens anzunehmen. Der Zertifizierungsausschuss, bestehend aus unabhängigen zertifizierten Experten, prüft die Empfehlung des Auditors und entscheidet über die Siegelvergabe. Hier greift das Multi-Augen-Prinzip. Die Prüfberichte, die sich daraus ergeben, sind öffentlich zugänglich und geben so zu jeder Zeit den Prüfungsumfang und das Prüfungsergebnis wieder.

BvD-News: Was haben Auftragnehmer und Auftraggeber konkret davon?

Dr. Niels Lepperhoff: Auftraggeber und Auftragnehmer profitieren durch die Zertfizierung in mehrfacher Hinsicht: Es fallen nur geringe Kosten für Datenschutzkontrollen an, es ergibt sich mehr Sicherheit durch zertifizierte Auftragnehmer und die Prüfung erfolgt unabhängig, transparent und offen nachvollziehbar.

BvD-News: Die Prüfung nehmen Auditoren ab. Einfach gefragt: Wie wird man zertifizierter Auditor?

Dr. Niels Lepperhoff: Wer sich als Auditor zertifizieren lassen möchte, muss bestimmte Bedingungen erfüllen. Dies haben BvD und GDD zur Bedingung gemacht, um dem hohen Anspruch des neu entwickelten Datenschutzstandards zur Auftragsdatenverarbeitung gerecht zu werden.

Dr. Niels Lepperhoff ist Geschäftsführer der von BvD und GDD neu gegründeten DSZ Datenschutz Zertifizierungsgesellschaft mbH.

Konkret bedeutet das: Zertifizierte Auditoren müssen über eine Ausbildung zum Datenschutzbeauftragten nach der zwischen dem BvD und der GDD abgestimmten Ausbildung von 2008 oder einer in Inhalt und Umfang vergleichbaren Ausbildung verfügen. Erwartet wird eine einschlägige Berufserfahrung als Datenschutzbeauftragter oder Mitarbeiter eines Datenschutzbeauftragten von mindestens sechs Jahren. Vier Jahre reichen bei vorliegendem Magister, Bachelor-Abschluss oder dem ersten juristischen Staatsexamen an einer staatlich anerkannten Hochschule aus. Wer zugelassen werden möchte, muss eine Ausbildung zum Auditor in einem beliebigen Feld oder Berufserfahrung als Auditor in einem beliebigen Feld vorweisen. Obligatorisch ist eine Teilnahme an der Fortbildung

zum Auditor nach DS-BvD-GDD-01, die ab Frühjahr 2014 von BvD und GDD angeboten werden. Weiterer Aspekt: Eine innerhalb der letzten zwölf Monate bestandene Prüfung zum Auditor nach DS-BvD-GDD-01. Erst dann kann der Auditor Prüfungen im Rahmen dieses Zertifizierungsprozesses durchführen.

BvD-News: Gibt es schon Datenschutzbeauftragte, die als Auditoren tätig werden können?
Dr. Niels Lepperhoff: Ja. Erste Auditoren sind zertifiziert, so dass Unternehmen ab sofort ein Siegel beantragen können.

BvD-News: Was haben externe Datenschutzbeauftragte als BvD-Mitglied davon, Auditor zu sein?
Dr. Niels Lepperhoff: Für den Auditor ergeben sich gewisse Vorteile: Er kann mit der Verleihung der Zertifizierung als Auditor werben und er wird in eine zentrale Auditorenliste eingetragen. Damit sich der Auditor regelmäßig weiterbildet und seine Unternehmensprüfungen stets auf dem neuesten Stand des Datenschutzstandards verlaufen, ist das Zertifikat drei Jahre ab Ausstellungsdatum gültig. Es kann jeweils um weitere drei Jahre verlängert werden, sofern die Zertifizierungsvoraussetzungen, wie nachgewiesene Fortbildungen, erfüllt werden.

Datenschutzkonforme Wege ins Web 2.0

Fortbildung Social Media für Datenschutzbeauftragte am 4. November

Am 4. November findet im NH Hotel Frankfurt-Mörfelden die ganztägige BvD Fortbildung „Social Media für Datenschutzbeauftragte“ statt. Wir werfen einen Blick auf die social media Basics und Twitter & co. Ebenso werden rechtliche Betrachtungen hinsichtlich der Mitarbeiter-Rekrutierung im Web, aber auch für das Marketing relevante Aspekte beleuchtet. Referenten für diese Fortbildung sind Christoph Heyn und Stefan Bachmann. Anmeldungen hierfür nimmt die Geschäftsstelle gerne entgegen.

ID|GARD

- Versiegelter Online-Speicher
- Sicherer Datenaustausch
- Team Workspaces
- Abhörsichere Nachrichten & Chat

ID|GARD

(abhör-) sicher kommunizieren in der Cloud

IDGARD beruht auf der weltweit einzigartigen Sealed Cloud Technologie. Sie stellt technisch sicher, dass nicht einmal der Anbieter des Dienstes Zugriff auf Daten oder Verbindungsinformationen hat. Durch Sealed Cloud erreichen Sie eine neue Dimension der Datensicherheit:

- Datenverarbeitung ohne Personenbezug
- Technisch garantierte Datentrennung
- Technisch garantierte Löschung!

Weitere Informationen unter www.idgard.de

Sie möchten IDGARD unverbindlich testen?
Schreiben Sie an business@idgard.de.

PRODUKT DES MONATS
2013
JUNI
Security-Insider.de

Datenschutz „Made in Germany?“

Dr. Stefan Brink über den neuen Stellenwert des Datenschutzes in der Gesellschaft und seine Auswirkung auf Datenschutzbeauftragte

Autor

Dr. Stefan Brink
Leiter Privater Datenschutz
Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34, 55116 Mainz
Tel. 06131 . 208-2449
E-Mail poststelle@datenschutz.rlp.de

Wir Datenschützer leben in stürmischen Zeiten. Das Thema Datenschutz ist in der Mitte der Gesellschaft angelangt, angesichts der heftigen Diskussionen der letzten Wochen muss man dem Datenschutz sogar „Wahlkampftauglichkeit“ attestieren. So schön es auch ist, nicht mehr am Rande der Gesellschaft ein Schattendasein führen zu müssen, und so beruhigend es ist, nicht mehr bei jedem zweiten Satz seine Existenzberechtigung in Frage gestellt zu sehen, so sehr macht das Sturmesbrausen um den Datenschutz aber doch eines deutlich: Jetzt ist es wichtiger denn je, den klaren Blick und mit ihm die Orientierung zu bewahren.

Zu diesem klaren Blick gehört dazu, dass vieles von der NSA-Affäre, von PRISM, TEMPORA und XKeyscore überhaupt nicht erstaunlich ist: Dass Geheimdienste spionieren, wussten wir schon vorher, und dass sie schon lange im Internetzeitalter angekommen sind, war ebenfalls allen klar. Geheimdienste agieren auch in und für Rechtsstaaten; auch die Tätigkeit der NSA wird durch Gesetze reguliert und von Gerichten kontrolliert. Dass es sich bei diesen Gerichten um „Geheimgerichte“ handelt, ist sicherlich mehr als ein Schönheitsfehler; aber auch in unserem Land weist die Kontrolle der Geheimdienste bekanntermaßen erhebliche Defizite auf. Die theoretisch bestehenden Kontrollmöglichkeiten der Verwaltungsgerichte werden faktisch dadurch unterlaufen, dass die Geheimdienste ihre wenigen gesetzlichen Unterrichtungspflichten gegenüber den Betroffenen gezielt übergehen. Die zum Ausgleich geschaffene parlamentarische Kontrolle ist offenkundig auch alles andere als effektiv. Mit dem grundrechtlich geschützten Anspruch der Bürgerinnen und Bürger, zu wissen, „wer was wann und bei welcher Gelegenheit über sie weiß“ und mit dem verfassungsverbürgten Recht, dies auch vor Gericht effektiv durchzusetzen, harmoniert diese Lage ganz und gar nicht. Auch in Deutschland nicht, auch das kommt uns an der NSA-Affäre bekannt vor.

Deutlich erstaunlicher ist demgegenüber, welche Angriffsziele sich die NSA ausgesucht hat: Es ist der Jedermann. Nicht mehr nur die Spionage gegenüber feindlichen Staaten und Institutionen, nicht mehr nur die altbekannte „freundliche Überwachung“ von befreundeten Staaten, jetzt wird der ganz durchschnittlichen Zivilbürger zum Ausforschungsobjekt des mächtigen Geheimdienstes. Der Informationshunger der Geheimdienste richtet sich damit erstmals gegen alle Staatsbürger – und soweit staatliche Restriktionen, das eigene Volk auszuspionieren, dem entgegenstehen, umgehen dies die Geheimdienste durch einen munteren Daten-Tauschhandel. Dies ist eine neue Qualität geheimdienstlicher Tätigkeit und wesentlich brisanter als der sattsam bekannte Umstand, dass Geheimdienste sich gerne dadurch nützlich machen, dass sie nebenbei auch noch Wirtschaftsspionage betreiben. Übrigens: Dies sollte ein letzter Weckruf gewesen sein für all die Unternehmen, die es für eine gute Idee halten, sich in Fragen der Datensicherheit von den Inlandsgeheimdiensten beraten zu lassen.

„Erstaunlich an der NSA-Affäre ist die Qualität der Ausforschung“

Warum aber wählte die NSA zum Angriffsziel den einzelnen Bürger? Weil sie es kann. Erstaunlich an der NSA-Affäre ist nämlich die Qualität der Ausforschungsleistungen, die darin besteht, erhebliche, wahrscheinlich sogar weit überwiegende Anteile der gesamten globalen Kommunikation ausforschen zu können. Dieses Unterfangen, das vor wenigen Jahren noch als größenwahnsinnig eingestuft worden wäre, scheint mit entsprechendem technischem Aufwand machbar geworden zu sein.

Auch damit ist jedoch noch nicht der Kern der

NSA-Affäre offengelegt. Ein Blick vor unsere Haustür lehrt uns, dass mit der Erhebung einer Flut von Daten noch nicht viel gewonnen ist. Gerade das Beispiel Videoüberwachung zeigt uns, dass der Übergang von analoger zu digitaler Technik in den vergangenen zehn Jahren zunächst einmal nichts anderes bewirkte, als ein Überquellen der – erschwinglich gewordenen – Datenspeicher. Entscheidend für die Überwachungsqualität war auch hier, dass der Überwachungsbetreiber nicht nur absurde Mengen von Bilddaten erheben kann, sondern dass er jetzt erstmals in der Lage ist, diese Datenflut auch intelligent auszuwerten. Erst mit der Entwicklung und Implementierung von Auswertungs-Software für Videoüberwachungen wird diese hochintensive Überwachungsform effektiv – und aus Sicht des Datenschutzes verstärkt kontrollbedürftig.

„Das Ende der anonymen Nutzungsmöglichkeiten ist besiegelt“

Eben dies scheint der NSA im Hinblick auf unsere Kommunikationsdaten auch gelungen zu sein, glaubt man den geleakten Dokumenten – und die NSA hat sich zwar lautstark über das Whistleblowing beschwert, aber nie ernsthaft in der Sache dementiert –, so besitzt die NSA jetzt effektive Auswertungsmöglichkeiten auch für diese Datenmengen.

Damit ist das Ende der anonymen Nutzungsmöglichkeit von Medien einschließlich des Internet und zugleich das Ende der Vertraulichkeit von Kommunikationsinhalten besiegelt. Dies vor allen Dingen deshalb, weil die Geheimdienste offensichtlich hinreichende Möglichkeiten haben, Zugangssicherungen zu überwinden und auch anspruchsvolle Verschlüsselungsmethoden zu kompromittieren. Hier wird es zwar auf absehbare Zeit zu einem Wettlauf zwischen Codierern und Decodierern kommen, ein relevanter Vorsprung wird sich jedoch nur für Hightech-Unternehmen und wenige staatliche Stellen erarbeiten lassen. Für den Otto-Normalverbraucher gilt jetzt und in Zukunft: Vertrauliche Kommunikation ist via Internet nicht mehr gewährleistet.

Dies sind nun wirklich stürmische Zeiten für den Datenschutz. Die seit Monaten im Tagesrhythmus neu verbreiteten Einsichten in die Fähigkeiten und Ziele der Geheimdienste verbreiten erhebliche Unruhe, ja Angst bei den Internet-Nutzern, also bei allen. Private, aber auch gewerblich Tätige wenden sich hilfesuchend an IT-Dienstleister, fragen den Aufsichtsbehörden ein Loch in den schmalen Bauch und pilgern in Crypto-Partys von Anbietern aller Couleur. Herrschte Anfangs noch Wut gegenüber der Übergriffigkeit der NSA, machte sich bald eine gefühlte Ohnmacht breit, die nach den Meldungen über die Fähigkeit der NSA, beliebige Verschlüsselungen zu knacken, der blanken Verzweiflung wich.

Dabei ist den meisten Internet-Nutzern das ganze Ausmaß dieser Affäre noch gar nicht ins Bewusstsein gedrungen. Auch wenn jede Internet-basierte Kommunikation in Zukunft von den Geheimdiensten durchforscht werden kann, so bleibt die Auswertung dieser Datenberge doch auch in Zukunft ein durchaus aufwändiges, aber gleichzeitig wenig ertragreiches Unterfangen. Viel bedrohlicher für den Einzelnen und seine informationelle Selbstbestimmung als die Suche der Geheimdienste nach der Stecknadel im Heuhaufen wird es sein, wenn die Sicherheitsbehörden einzelne Bürger „zur Stecknadel erklären“. Sobald Sicherheitsbehörden auf welcher Grundlage auch immer Einzelpersonen als betrachtenswert einstufen und durchleuchten wollen, helfen ihnen strategische Überwachungsmaßnahmen kaum weiter. Hier greifen sie vielmehr auf jene Datenlager zu, die der Großteil der „sicherheitsrelevanten Bevölkerung“ (also aller Einwohner unter 35 Jahren) bereits angelegt haben: auf Facebook, Google Plus, Skype und Twitter. Die dort zunächst unter wirtschaftlichen Gesichtspunkten erschaffenen Persönlichkeitsprofile sind das ideale Angriffsziel aller Sicherheitsbehörden. Die innerstaatlichen gesetzlichen Grundlagen reichen allemal für einen behördlichen Zugriff aus, so dass es auf eine besondere Kooperationsbereitschaft der Plattformbetreiber überhaupt nicht mehr ankommt.

„Die Datenschutz-Grundverordnung steht offenkundig vor dem Scheitern“

Seit geraumer Zeit tragen sich Datenschützer mit dem Gedanken, dass in einem „Rückzug auf die Festung Europa“ eine geeignete Reaktion auf die transatlantischen Angriffe auf unsere Privatsphäre liegen könnte. Wichtige Aspekte der Datenschutzpolitik der europäischen Kommission basieren gerade auf der Zielsetzung, außereuropäische Wirtschaftsunternehmen unter das europäische Datenschutzregime zu zwingen und sie ansonsten

vom attraktiven europäischen Markt auszuschließen. Wer Waren oder Dienstleistungen in der Union anbieten möchte, soll den europäischen Datenschutzregeln auch dann unterworfen werden, wenn er keine Niederlassung innerhalb der EU hat und die Datenverarbeitung außerhalb des räumlichen Anwendungsbereichs der Datenschutzgrundverordnung durchführt (Art. 3 Ziff. 2 des Entwurfs zur Datenschutz-Grundverordnung).

Allein, die Datenschutz-Grundverordnung steht offenkundig vor dem Scheitern. Während das Europäische Parlament in einer Flut von mehreren Tausend Änderungsanträgen unterzugehen droht, ist eine Konsensfindung innerhalb des Rates noch nicht einmal in Ansätzen zu erkennen. Kaum ein Artikel, zu dem nicht wenigstens ein Mitgliedstaat grundsätzliche Bedenken angemeldet hat, Kompromisslinien sind nicht in Sicht, kein realistischer Fahrplan für den Trilog. Auf die deutlichen inhaltlichen Schwächen des Verordnungsentwurfs, insbesondere auf die von Deutschland aus heftig kritisierte Abkehr vom Modell des betrieblichen Datenschutzbeauftragten, wird man kaum noch eingehen müssen.

„Festung Europa“, unter dieses Schlagwort kann man auch eine Erklärung einordnen, welche die Konferenz der Datenschutzbeauftragten von Bund und Ländern im Juli 2013 angesichts der NSA-Affäre fasste. Die Konferenz kündigt darin an, bis zu einem effektiven Schutz der Bürger vor den Geheimdiensten „werden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten (z. B. auch zur Nutzung bestimmter Cloud-Dienste) erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind“. Die Schärfe der damit im Raum stehenden Drohung ist kaum zu überbieten, die Datenschützer kündigen nichts weniger als die mögliche Beendigung des transatlantischen Datenaustauschs an. Was das für die gegenseitigen Wirtschaftsbeziehungen bedeuten würde, kann sich jeder unschwer ausmalen. Zwar sind sich Datenschützer schon seit langem darin einig, dass das Safe-Harbor-Abkommen kaum mehr als „weiße Salbe“ auf jener Wunde ist,

Datenschützer müssen sich auf ihre Grundlagen zurückbesinnen, sagt Dr. Stefan Brink.

die sich Europa selbst dadurch zufügte, dass es seine datenschutzrechtliche Überzeugung auf dem Altar der (amerikanischen) Wirtschaft opferte. So unverblümt die blinden Flecke dieses Abkommens anzusprechen zeugt zugleich vom Mut der verzweifelten Datenschützer, die drohend ihre stärkste – und letzte - Karte ziehen. Der US-amerikanische Verteidigungsminister Caspar Weinberger sagte einst zur Politik der atomaren Abschreckung: „Diese Politik ist paradox, aber sie hat einen Vorteil: Sie funktioniert!" Hoffen wir es.

„Die deutsche Datenschutzkultur hat durchaus ihre Strahlkraft"

Letzte Rückzugsposition: „Deutscher Datenschutz". Vor dem Hintergrund der geschilderten internationalen und europäischen Entwicklung nimmt es nicht Wunder, dass nunmehr verstärkt der Ruf nach einem Datenschutz „Made in Germany" zu vernehmen ist. Dahinter steht häufig die durchaus attraktive Idee, das hohe deutsche Datenschutzniveau in einen Wettbewerbsvorteil umzumünzen. Teilweise scheint dies, wie das Beispiel „German Cloud" belegt, auch zu gelingen. Die deutsche Datenschutzkultur, die im Wesentlichen von einem engmaschigen Netz qualifizierter betrieblicher Datenschutzbeauftragter, aber ebenso von Aufsichtsbehörden getragen wird, die einerseits fachkundig beraten, andererseits aber auch sanktionieren können, hat durchaus ihre Strahlkraft.

Aber auch hier sollte sich niemand von falschen Vorstellungen die Orientierung nehmen lassen. Offensichtlichen Erfolgen der Datenschützer sogar im internationalen Bereich – erinnert sei an die „deutsche Version" von Google-Streetview oder die Abschaltung der Gesichtserkennung bei Facebook – stehen ebenso „überzeugende" Defizite entgegen: Da ist im Bereich der Exekutive an erster Stelle ein Innenminister zu nennen, der mit seinem denkwürdigen Vorschlag zu einem „Supergrundrecht auf Sicherheit" Verfassungsjuristen erstaunte und Datenschützer frustrierte. Da ist eine nationale Gesetzgebung, der es seit mehr als zehn Jahren nicht gelingt, die Datenschutzvorschriften ins Internetzeitalter zu transponieren und die mit ihrem wichtigsten Datenschutzprojekt, dem Beschäftigtendatenschutzgesetz, sang- und klanglos gescheitert ist. Und schließlich ist da eine Rechtsprechung, die mit der Thematik Datenschutz immer wieder fremdelt. Der BGH wendet geltendes Datenschutzrecht nicht an (Spickmich.de-Entscheidung), der Bundesfinanzhof entmutigt Unternehmer, die sich datenschutzkonform verhalten wollen (Entscheidung zur AEO-Zertifizierung) und viele Arbeitsgerichte übersehen immer noch, dass mit § 32 BDSG eine gültige streitentscheidende Norm ihrer Anwendung harrt. Datenschutz „Made in Germany"? Da gibt es mehr Anlass für Selbstkritik als für Selbstzufriedenheit.

Heißt es am Ende also, dass das „Projekt Datenschutz" vor dem Scheitern steht? Natürlich nicht. Aber es heißt, dass sich in stürmischen Zeiten wie diesen die Datenschützer auf ihre Grundlagen zurückbesinnen müssen. Und da gilt: Datenschützer sein heißt standhaft zu bleiben. Standhaft angesichts einer Übermacht von Gegnern, die ihre Angriffe aus wirtschaftlichen, zeitgeistgebundenen (erinnert sich eigentlich noch jemand an die Post Privacy-Debatte?) und überwachungsstaatlichen Motiven heraus betreiben. Standhaft zu bleiben, nicht um im Wege zu stehen, sondern um eine Position zu verteidigen und zu schützen, die wir Deutsche im vergangenen Jahrhundert mehrfach gelernt und überwiegend auch begriffen haben: Dass das Grundrecht auf informationelle Selbstbestimmung seine Berechtigung hat und jede Mühe lohnt. Und zu diesem Markenkern zählt das generelle Verbot der Datenverarbeitung mit Erlaubnisvorbehalt – und nicht ein „risikoorientierter Datenschutz" nach Kassenlage – dazu zählt die freie und ausdrückliche Einwilligung, dazu zählen qualifizierte und einflussreiche betriebliche Datenschutzbeauftragte genau so wie unabhängige und durchsetzungsfähige Aufsichtsbehörden.

Ermutigen sollte uns dabei, dass mit diesem Datenschutzverständnis - anders als häufig verlautbart - kein „deutscher Sonderweg" beschritten wurde, sondern eine auch international durchaus anschlussfähige Grundentscheidung getroffen wurde. Mittlerweile ist das „right to privacy" nicht nur in Art. 12 der UN-Menschenrechtserklärung und in Art. 8 der Europäischen Menschenrechtskonvention verankert, sondern auch in Art. 7 und 8 der EU-Charta der Grundrechte zum geltenden europäischen Recht erwachsen. Dass diese Grundrechtsposition im Einzelfall schwer durchzusetzen ist, kann uns Datenschützer kaum schrecken; Stichwort: Standhaftigkeit. Für Resignation besteht daher zwar hin und wieder Anlass, in der Sache aber kein Grund.

„Optimistisch, dass es bis April 2014 eine Einigung gibt“

Im Interview nimmt MdEP Jan Philipp Albrecht Stellung zu Zeitplan und inhaltlichen Auseinandersetzungen auf dem Weg zur EU-DSGVO

Die Ausgestaltung der EU-DSGVO ist weiterhin Gegenstand zahlreicher Diskussionen auf nationaler und europäischer Ebene. Im Interview mit BvD-Vorstand Rudi Kramer erläutert Jan Philipp Albrecht (Grüne), im zuständigen Ausschuss LIBE (Bürgerliche Freiheiten, Justiz und Inneres) als Berichterstatter des Ausschusses für die Meinungsbildung verantwortlich, seine Position zu Terminen, Inhalten und den Auswirkungen der Bundestagswahl auf den weiteren Prozess.

BvD: Herr Albrecht, glauben Sie heute, dass es eine Einigung über die EU-DSGVO bis April 2014 im Trilogverfahren geben wird?

Jan Philipp Albrecht: Ich bin da sehr optimistisch, dass es eine Einigung vor der Europawahl im Mai 2014 geben wird, wenn der politische Wille im Ministerrat da ist. Die Äußerungen der letzten Wochen einzelner Mitgliedsstaaten lassen darauf schließen, dass auch der Ministerrat diesbezügliche Prioritäten setzt, um bis November eine Position für das Trilogverfahren abgestimmt zu haben. Die letzte Sitzung des Europäischen Parlaments in dieser Legislaturperiode findet im April in Straßburg statt.

BvD: Die Positionen im Parlament und auch im Rat waren im Frühsommer nach den Berichten noch sehr weit auseinander - was hat sich über den Sommer geändert?

Jan Philipp Albrecht: Über den Sommer wurde deutlich, dass es einige Mitgliedsstaaten gibt, die großes Interesse an einem einheitlichen Datenschutz in Europa haben. Auch die Bundesrepublik hat durch die Vorgänge um PRISM gemerkt, dass es wichtig ist, das hohe Datenschutzniveau in Deutschland und das Vertrauen der Bürgerinnen und Bürger in ihre Souveränität über die Datenverarbeitung aufrechtzuerhalten.

BvD: Inwieweit wird sich nach Ihrer Einschätzung das Ergebnis der Bundestagswahl auf die deutsche Position im weiteren Verfahren auswirken?

In der BvD-Infoveranstaltung in Brüssel – hier neben BvD-Vorstand Dr. Jens Eckardt – hob Jan Philipp Albrecht hervor, wie wichtig den EU-Parlamentariern der Input durch Fachleute ist.

Auch beim Infotag des BvD im vergangenen Jahr in Brüssel stellte Jan Philipp Albrecht seine Ansicht dar. Für die Eingaben des BvD waren er und Alexander Alvaro sehr dankbar.

Jan Philipp Albrecht: Das Ergebnis der Bundestagswahl selbst wohl nicht, aber eher die Besetzung des Innenministeriums ist entscheidend, mit welchen Vorgaben die Verhandlungsführung ausgeübt wird. Der Bundesminister des Innern Hans-Peter Friedrich hat während seiner Amtszeit gezeigt, dass ihm der Datenschutz nicht am Herzen liegt. Statt sich in der Grundverordnung für ein hohes Niveau stark zu machen, hat er durch Verzögerung und Selbstregulierungsvorschlägen den großen US-Internetkonzernen in die Hände gespielt.

BvD: In der EU-DSGVO werden Definitionen zu Pseudonymisierung und Verschlüsselung geregelt. Diese beiden Themen werden in Fachkreisen sehr kontrovers diskutiert, da sie jeweils abhängig von sich laufend ändernden technischen Entwicklungen zu sehen sind. Ist diese Definition unabhängig davon?
Jan Philipp Albrecht: Es ist unser Anspruch, hier bei beiden Themen eine Formulierung zu finden, die technikneutral ist und bleibt.

BvD: Sieht die derzeitig diskutierte Fassung eine IP-Adresse als personenbezogenes Datum?
Jan Philipp Albrecht: Der Grundsatz muss heißen: im Zweifel für den Schutz der Person. Anders ist ein konsequenter Schutz auch nicht denkbar. Bei IP-Adressen kann ein Unterschied gemacht werden, durch wen diese verwendet werden, sei es eine natürliche Person oder ein Unternehmen – der Empfänger dieser IP-Adresse muss jedoch zunächst immer davon ausgehen, dass es sich um eine natürliche, schutzwürdige Person handelt. Anders wäre beispielsweise auch der hervorgehobene Schutz von Kindern bei der Datenverarbeitung nicht umsetzbar. Wir versuchen dies in dem Erwägungsgrund 24 darzustellen.

BvD: Welche Auswirkung hat die Änderung von „must" in „shall" in den Grundsätzen der Datenverarbeitung des Art. 5 im ersten Satz? Relativieren sich die Vorgaben nicht dadurch?
Jan Philipp Albrecht: Diese Änderung stellt nur eine linguistische Anpassung dar und ist keine inhaltliche Relativierung des Geltungsbereiches. Das „must" war sprachlich einfach falsch.

BvD: Welche Vorteile wird ein Unternehmen haben, wenn es - freiwillig oder über eine Bestellpflicht - einen betrieblichen DSB bestellt?
Jan Philipp Albrecht: Konkret sind Vorteile bei der vorherigen Zurateziehung vorgesehen. Hier kann der betriebliche Datenschutzbeauftragte die Abstimmung mit der Aufsichtsbehörde ersetzen. Durch seine Fachkunde und Branchenkenntnis ist zu erwarten, dass er die Interessen der betroffenen Personen bei den entsprechenden Fragen ebenso berücksichtigen kann wie eine Aufsichtsbehörde – nur schneller, insbesondere bei Rückfragen oder sich erst entwickelnden Sachverhalten. Weiterhin ist im Gespräch, dass die Bestellung eines betrieblichen Datenschutzbeauftragten auch bei einer PIA (Private Impact Assessment – Datenschutzfolgenabschätzung) Vorteile bringen kann.

BvD: Reichen diese Vorteile aus, um die kritischen Staaten im Ministerrat zu überzeugen?
Jan Philipp Albrecht: Wir haben schon heute Rückmeldungen von internationalen Unternehmen, welche die Vorteile hervorheben, die ein betrieblicher Datenschutzbeauftragter in Deutschland bei der Meldepflicht und der Vorabkontrolle bringt, weil diese Prozesse intern gelöst werden können. Zudem ist es einfacher, eine kritische Fragestellung intern mit einem kompetenten Ansprechpartner zu erörtern, als schriftlich mit einer Aufsichtsbehörde. Die Nichtbestellung eines Datenschutzbeauftragten befreit ja nicht von den sonstigen Aufgaben und Pflichten einer für die Verarbeitung verantwortlichen Stelle. Dies nehmen auch zunehmend die Mitgliedsstaaten zur Kenntnis.

Im Interview mit BvD-Vorstand Rudi Kramer stellt Jan Philipp Albrecht den weiteren Zeitplan zur Verabschiedung der EU-DSGVO vor. (Fotos: Michael Braun)

BvD: An wen kann ich als betroffene Person in einem Unternehmen vertrauensvoll wenden, das keinen DSB hat?

Jan Philipp Albrecht: Da bleibt dann natürlich nur das Unternehmen selbst oder dessen Aufsichtsbehörde. Die Möglichkeit sich an jemanden innerhalb des Unternehmens zu wenden, der einer Verschwiegenheitspflicht unterliegt ist, sei es als Kunde oder Lieferant, dann nicht mehr möglich. Alternativen könnten Verbraucherschutzorganisationen darstellen. Aber auch Beschäftigte hätten bestenfalls nur noch eine Arbeitnehmervertretung, sofern es in dem Unternehmen eine gibt.

BvD: Auch Staaten, die sonst Selbstregulierung propagieren, sprachen sich gegen einen DSB aus - was hat diese nicht überzeugt?

Jan Philipp Albrecht: Gute Frage, weil die Staaten, die mit Elementen der Selbstregulierung gute Erfahrungen gemacht haben, die Selbstregulierung durchaus befürworten. Nicht zuletzt spricht eine qualitative Fachkunde bei betrieblichen Datenschutzbeauftragten auch nur für die Selbstregulierung in diesem Bereich.

BvD: Wo sehen Sie persönlich inhaltlich den Knackpunkt, das erzielte Ergebnis nicht mehr als Erfolg zu betrachten?

Jan Philipp Albrecht: Maßstab sind die Grundlagen aus der RL EU 95/46 EG. Diese stellt eine Art „rote Linie“ dar, an der sich der inhaltliche Erfolg der EU-DSGVO messen lassen muss. Hinzu kommt, dass die EU-DSGVO einen höheren Sanktionsrahmen und insgesamt mehr Durchsetzungsmöglichkeiten bieten wird, als bisher unter der Richtlinie und auch in Deutschland möglich war. Derzeit entspricht der Verhandlungsstand aber nahezu durchgehend dem Standard des deutschen Datenschutzrechts und geht in Teilen sogar darüber hinaus, daher bin ich zuversichtlich.

BvD: Bei der EU RL95/46 EG lag der Zeitraum zwischen dem Entwurf der Kommission und der endgültigen Einigung bei ca. 5 Jahren, warum sollte es bei der Verordnung in nur zwei Jahren klappen?

Jan Philipp Albrecht: Bei der Richtlinie musste das Thema Datenschutz auf der europäischen Bühne erst erarbeitet werden, das Bewusstsein bei vielen Akteuren geschaffen und die Definitionen abgestimmt werden. Dieser grundsätzliche Teil entfällt nun. Auch sind durch die vorherigen Konsultationsverfahren der EU-Kommission zur Überarbeitung der RL EU 95/46 EG Anregungen im Vorfeld bereits bewertet bzw. berücksichtigt worden.

BvD: Ziel der europäischen Aktivitäten war eine gleichmäßigere rechtliche Gestaltung innerhalb der EU. Wo sehen Sie nach dem derzeitigen Verhandlungsstand die gravierendsten Veränderungen zur aktuell bestehenden Rechtslage in Deutschland?

Jan Philipp Albrecht: Es sind durch den Entwurf der Kommission und die nachfolgenden Verhandlungen bestimmte Schlagworte in der Öffentlichkeit diskutiert worden, die hängen bleiben werden wie bei der Datenportabilität, dass ich als Betroffener

meine Daten auch anderweitig zur Nutzung erhalten kann oder der Durchsetzung des Löschungsanspruchs durch das Schlagwort „Recht auf Vergessen“. Für das allgemeine Datenschutzniveau in Deutschland erwarte ich nach dem aktuellen Verhandlungsstand keine gravierenden Veränderungen der Rechtslage in Deutschland

BvD: Das Bild der EU wird für viele geprägt durch Schuldenkrisen, Intransparenz bei Entscheidungen und fehlender Praxisnähe - halten Sie die EU-DSGVO geeignet, der wachsenden europäischen Skepsis der Bürger entgegenzuwirken?

Jan Philipp Albrecht: Ich finde, dass gerade die digitale Kommunikation, die grenzüberschreitende Verarbeitung personenbezogener Daten, die europaweite Nutzung elektronischer Medien den Menschen deutlich macht, welch ein Vorteil in einer einheitlichen, europaweiten Regelung liegen kann. Hierauf fußt das Vertrauen in die Rechtssicherheit. Egal, wo in Europa ich mich aufhalte und Datenspuren hinterlasse - ich muss mir nicht alle paar 100 km überlegen, ob hier mit meinen Daten mehr gemacht werden kann als im Nachbarland. Diese Rechtssicherheit ist nicht nur für die Unternehmen und die Wirtschaft eine erhebliche Erleichterung, sondern auch für den Nutzer, den Konsumenten, den Menschen und sein Recht auf informationelle Selbstbestimmung.

BvD: Was empfehlen Sie Bürgern, die ihre Privatsphäre bewahren möchten? Verzicht auf elektronische Medien oder ist die Privatsphäre bei der Verwendung von elektronischen Kommunikations- und Navigationsmitteln nicht mehr zu gewährleisten?

Jan Philipp Albrecht: Generellen Verzicht zu empfehlen ist der falsche Weg. Ich nehme auch noch am Straßenverkehr teil, obwohl ich die Unfallstatistiken kenne. Es sollte daher nicht nur der Anspruch der Politik sein, den Bürgern die Nutzung digitaler Medien zu ermöglichen. Die Politik muss die Bürger auch in die Lage versetzen, die Informationen, die sie für die Entscheidung, ob, wie und zu welchem Preis sie diese Medien nutzen, auch zu erhalten und sie befähigen, diese Entscheidung selbst zu treffen.

RHENUS LOGISTICS

RHENUS OFFICE SYSTEMS

Archivierung mit Sicherheit

Ihr verlässlicher Partner für kostenoptimierte Archivierung in Hochsicherheitsarchiven.

Rhenus Office Systems ist spezialisiert auf Dokumenten- und Informationslogistik. Mit deutschlandweit 13 Archiven und einem flächendeckenden Vertriebsnetz sind wir auch in Ihrer Nähe. Sprechen Sie uns an – Wir helfen Ihnen, Kosten einzusparen und Platz zu schaffen.

Ihre Akten sind bei uns Zuhause!

OFFICE SYSTEMS

Rhenus Office Systems GmbH · Rhenus-Platz 1 · 59439 Holzwickede
Telefon: +49 (0)2301 29-1600 · Fax: +49 (0)2301 29-1593
info.ros@de.rhenus.com · www.office-systems.de

Datenschutz-Prüfungsaktion des BayLDA im Jahr 2013

Fragebogen zur Erhebung datenschutzrelevanter Angaben

Oft wird von vielen Seiten bemängelt, die datenschutzrechtlichen Aufsichtsbehörden seien personell zu schlecht ausgestattet, um auch eine effektive, anlasslose Kontrolle bei verantwortlichen Stellen durchzuführen. Dieser Situation begegnen die Aufsichtsbehörden zunehmend mit einer eigentlich ungewöhnlichen Methode: einem Fragebogen. So wurden in Hamburg beispielsweise Fragebogen zur Videoüberwachung durch öffentliche Stellen oder zum Datenschutzmanagement bei nicht-öffentlichen Stellen eingesetzt (vgl. z.B. Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit für die Jahre 2012/2011) oder der Einsatz eines Fragebogens auf bestimmte Branchen beschränkt, wie in Rheinland-Pfalz auf Hotelbetriebe (vgl. die Pressemeldung des LfDI Rheinland-Pflanz vom 30.4.2013). Auch durch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) wurde in 2013 ein Fragebogen eingesetzt. Oberregierungsrat Manfred Ilgenfritz, Referatsleiter im BayLDA, leitete und koordinierte diese aufsichtsrechtliche Maßnahme und berichtet hierüber. Der Fragebogen ist in aktualisierter Form auf den Webseiten des BvD hinterlegt (https://www.bvdnet.de/bvd-news-links.html, siehe auch QR-Code links). Er kann durch Datenschutzbeauftragte auch außerhalb Bayerns zur Eigenkontrolle verwendet werden, mit welchen Fragestellungen man bei Prüfungen durch Aufsichtsbehörden rechnen kann oder auch zur Vorbereitung eines internen Audits dienen.

Download

Fragebogen des BayLDA

So geht's: Einfach QR-Code mit Smartphone oder Tablet einscannen.

Es heißt ja: „Vertrauen ist gut, Kontrolle ist besser". Nach diesem Prinzip sieht § 38 Abs. 1 Satz 1 BDSG bei den nicht-öffentlichen Stellen eine Kontrolle der Ausführung des BDSG sowie anderer Vorschriften über den Datenschutz durch die Aufsichtsbehörden vor.

In der Praxis stellt sich für Aufsichtsbehörden hierzu die Frage, wie am Besten möglichst viele und effektive Kontrollen rationell durchgeführt werden können, um eine gewisse Breitenwirkung zu erzielen. Vor-Ort-Prüfungen in den Unternehmen, bei Freiberuflern, bei Vereinen usw., sind zweifellos am wirkungsvollsten, beanspruchen aber mit Vorbereitung, Außendiensttermin und Nachbearbeitung sehr viel Zeit. Deshalb führen Aufsichtsbehörden häufiger auch Kontrollen mittels schriftlicher Abfrageaktionen durch.

Das BayLDA, die Aufsichtsbehörde nach § 38 BDSG für Bayern, hat insoweit im Januar 2013 eine größer angelegte Kontrolle bei über 150 Unternehmen gestartet. Aus einem Internetportal der Vereinigung der Bayerischen Wirtschaft e.V. wurden nach dem Zufallsprinzip stichprobenmäßig ca. 100 Unternehmen verschiedener Branchen und Größe ausgewählt. Zusätzlich wurden etwa 50 Bankinstitute mit einbezogen.

Die Unternehmen erhielten ein Schreiben mit Info-Blättern und einem Fragenkatalog zugesandt, den sie innerhalb einer 6-Wochen-Frist mit Vorlage der relevanten Dokumente beantworten sollten.

Dieser Fragenkatalog betraf hauptsächlich
• die Erlaubnis-Rechtsvorschriften für die

Per Fragebogen hat das BayLDA datenschutzrelevante Angaben erhoben.

Autor

Manfred Ilgenfritz
Referatsleiter im Bayerischen Landesamt für Datenschutzaufsicht (BayLDA), Promenade 27 (Schloss), 91522 Ansbach, www.lda.bayern.de

Erhebung, Verarbeitung und Nutzung personenbezogener Daten, auf die sich das betreffende Unternehmen stützt,
- den Datenschutzbeauftragten, seine Stellung und seine konkrete Tätigkeit,
- die Vorlage des öffentlichen Verfahrensverzeichnisses,
- die Verpflichtungen auf das Datengeheimnis,
- die Vorlage der Verträge über Auftragsdatenverarbeitung,
- ausgewählte Punkte zum Beschäftigtendatenschutz, wie die Regelungen zur privaten Nutzung von Internet und E-Mail und zur Verwendung privater Kommunikationsmittel am Arbeitsplatz,
- die Videoüberwachung, einschließlich der konkreten Zweck-Festlegungen im Sinne von § 6b Abs. 1 Nr. 3 BDSG,
- die bestehenden Regelungen zur Sperrung bzw. Löschung von Daten,
- die Vorlage des Konzepts zu den getroffenen technischen und organisatorischen Maßnahmen nach § 9 BDSG und der Anlage zu § 9 BDSG,
- den Maßnahmenplan für eventuelle Datenpannen nach § 42a BDSG.

Nach Ablauf der Frist hatten sich nur neun der angeschriebenen Unternehmen noch nicht gemeldet, die aber dann nach einer Anmahnung reagiert haben.

5 Prozent der Geprüften setzen Datenschutz jetzt erst um

Etwa 5 Prozent der insoweit Geprüften (kleine und mittlere Größenordnungen) haben aufgrund unseres Prüfungsanschreiben erst mit der Datenschutzumsetzung im Sinne der gesetzlichen Anforderungen begonnen.

Der größere Teil der Unternehmen hatte schon einige grundlegende Vorgaben aus dem BDSG erfüllt, wie die Bestellung eines Datenschutzbeauftragten oder die Verpflichtung der Beschäftigten auf das Datengeheimnis, es gab aber noch deutliche Lücken bei der Umsetzung des BDSG, die erst aufgrund des Prüfungsanschreibens aufgearbeitet wurden. Nur bei wenigen Unternehmen konnte die Prüfung ohne jede Anmerkung abgeschlossen werden.

Mängel waren häufiger festzustellen bei:
- der Bestellung und Tätigkeit des Datenschutzbeauftragten, z. B. nicht vertretbare Interessenkollision (Datenschutzbeauftragter gleichzeitig DV-Administrator, Personalchef, Vorstand oder ähnliches), wenig Aktivität als Datenschutzbeauftragter,
- der Videoüberwachung ohne schriftliches Konzept (siehe dazu z. B. aktuell im Urteil des BGH vom 24.5.2013, V ZR 220/12),
- der ungeregelten Gestattung der privaten Internet- und E-Mail-Nutzung oder des Einsatzes privater DV-Technik am Arbeitsplatz,
- der Erstellung des im BDSG vorgesehenen öffentlichen Verzeichnisses der DV-Verfahren,
- fehlenden bzw. unzureichenden Verträgen zu Auftragsdatenverarbeitung.

Inzwischen ist die Prüfungsaktion zu etwa 75 Prozent abgeschlossen, im verbleibenden Rest sind noch Kritikpunkte aufzuarbeiten. In Einzelfällen werden von uns im Nachgang noch Vor-Ort-Prüfungen stattfinden, um nicht nur auf schriftliche Antworten und Unterlagen vertrauen zu müssen.

Das Ergebnis dieser aufsichtlichen Kontrolle im schriftlichen Verfahren hat uns gezeigt, dass solche Prüfungsaktionen eine gut geeignete Möglichkeit sein können, um in kürzerer Zeit eine größere Zahl von Unternehmen, Freiberuflern, Vereinen etc. zu erreichen. Wir planen deshalb für die Zukunft, weitere solche Prüfungsaktionen durchzuführen. Die Zufallsauswahl der in eine Prüfungsaktion einbezogenen Stellen wird dabei einerseits relevante Branchen mit umfangreicherer oder kritischer Verarbeitung personenbezogener Daten betreffen, darüber hinaus aber auch wieder die gesamte Breite der Wirtschaft erfassen. Unser Hauptziel ist dabei, durch Information und Beratung einen gesetzeskonformen Umgang mit den persönlichen Daten von Mitarbeitern, Kunden, Mandanten, Patienten usw. sowie eine angemessene Datenschutz- und Datensicherheitsorganisation zu erreichen und dadurch die Anzahl der Datenschutzbeschwerdefälle bei uns zu reduzieren.

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 fachlichen 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.

Weiter 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.

„Transparenz, aber kein Zugriff für alle“

Gerhard Friederici, Datenschutzbeauftragter für die Rhenus Office Systems, über die sichere Archivierung von Informationen

Die Diskussion um die Geheimdienstoperationen wie PRISM oder Tempora hat das Thema Datenschutz noch stärker in den Blick der Öffentlichkeit geführt. Dazu kommen Datenpannen in Unternehmen, die bei den betroffenen Unternehmen nicht nur zu einem Imageverlust, sondern im Zweifelsfall auch zu Vertragstrafen oder Regressansprüchen führen. Wie man Informationen sicher archiviert und wie ein ganzheitlicher Umgang mit Daten aussehen kann, hat BvD-News-Redakteur Michael Braun mit Gerhard Friederici, dem Datenschutzbeauftragten der Rhenus Office Systems, im Interview diskutiert.

BvD: Jeder Privatperson, aber auch jeder Behörde und jedem Unternehmen ist nicht erst seit der NSA-Affäre bewusst, dass die Sicherheit der eigenen Daten ein hohes Gut darstellt. Mit der Umsetzung dieses Wissens scheint es aber doch noch oft zu hapern?

Gerhard Friederici: Wenn wir an die in diesem Sommer in weiten Teilen der Öffentlichkeit geführten und dabei sehr lebhaften Diskussionen um die Überwachungsprogramme und Geheimdienstoperationen wie PRISM oder Tempora denken, dann kann ich aus Sicht eines Datenschützers das generell vorhandene Interesse für diese Fragen absolut bestätigen. Auch in den Gesprächen mit unseren Kunden ist das immer wieder ein Thema. Niemand möchte, dass private Informationen oder Firmeninterna in die Hände unberechtigter Dritter geraten. Richtig ist aber auch, dass zwischen diesem Anspruch, der Teil unseres Grundrechteverständnisses ist, und der lückenlosen Verwirklichung in vielen Fällen noch eine Lücke klafft.

BvD: Diese Unsicherheiten beginnen oft schon bei der Festlegung der Zugriffsberechtigung für bestimmte Akten und enden bei der unsachgemäßen Entsorgungen nicht mehr benötigter Unterlagen.

Gerhard Friederici: Richtig. Angesichts der Folgen von Datenpannen, die neben dem Imageverlust hohe Vertragsstrafen, Regressansprüche und somit in der Konsequenz auch den Verlust von Marktanteilen für ein Unternehmen bedeuten können, empfiehlt sich ein ganzheitlicher Ansatz für das Informationsmanagement. Denn Sicherheitslücken können an vielen Stellen auftreten. Aus Unkenntnis der gesetzlichen Regelungen, fehlender Zeit der damit betrauten Personen oder knappen Platzressourcen für diese Aufgaben ergeben sich vielfach Lecks, die hinterher kaum mehr zu schließen sind. Als Dokumentenlogistiker denken wir die Anforderungen in Prozessschritten und definieren für jede einzelne Maßnahme die in ihr gültigen Qualitätsstandards, die den datenschutzkonformen Umgang mit den Akten und Datenträgern gewährleisten können.

BvD: Datenpannen durch fehlendes Know-how und durch Spionage erlittene Datenverluste sind die eine Seite der Medaille, die im Archivwesen gebundenen Ressourcen von Personal und Räumlichkeiten die andere, oder?

Gerhard Friederici: Meiner Ansicht nach kann man sogar von vier Dimensionen sprechen, die zum Teil ineinander übergehen. Erstens sind dies alle Anforderungen, die mit einer physischen Archivierung verbunden sind. Zweitens sind dies alle Aufgaben, die mit dem Management von digitalem Archivgut verbunden sind. Es ist eben ein Unterschied, ob Sie es mit einem Aktenordner zu tun haben oder ob Sie beispielsweise für einen Webshop-Betreiber online abgeschlossene Vertragsverhältnisse revisionssicher verwalten und dokumentieren können. Hinzu kommen die beiden von Ihnen bereits kurz angerissenen Dimensionen. Also drittens der Schutz der Informationen vor fremdem Zugriff durch Wirtschaftskriminalität oder Unachtsamkeit. Und viertens die interne Arbeitsorganisation, um Papiere und Dateien für ihre

Info

Gerhard Friederici
ist Datenschutzbeauftragter für die Rhenus Office Systems 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.

Weiterbearbeitung in der Behörde oder im Unternehmen schnell und vollständig bereitzustellen. Das Bild vom allwissenden Archivar im Backoffice hat sich im Informationszeitalter ein wenig überlebt. Effiziente und dabei gleichzeitig sichere Strukturen, gerade auch mit Blick auf den Zugriff von verschiedenen geografischen Punkten aus, sind heute erforderlich.

BvD: Das Verhältnis zwischen Sicherheit und Transparenz stellt in unseren Tagen einen schwierigen Balanceakt dar.
Gerhard Friederici: Ganz genau. Die unsachgemäß entsorgten Patientenakten, die in der Papiertonne eines Krankenhauses landen, geben Auskunft über Dinge, die keinen Unbeteiligten etwas angehen. Hingegen ist bei der Konzeption, Ausgestaltung und Optimierung eines datenschutzkonformen Dokumentenmanagements Transparenz eine sehr wichtige Voraussetzung. Nur wenn alles offen besprochen wird, können auch potentielle Lücken in der Prozesskette geschlossen werden. Deshalb muss zum Beispiel geklärt werden, wer bestimmte Räume betreten darf, in denen schützenswerte Informationen vorhanden sind, und über die erforderlichen Schlüssel oder Codekarten für Aktenschränke verfügen kann. Jeder Person sind somit nur solche Zugriffsmöglichkeiten gestattet, wie sie vom Gesetzgeber allgemein und von den Datenschützern der verantwortlichen Stelle im jeweiligen Einzelfall zuvor festgelegt worden sind. So können sich unter Umständen im Intranet eines Unternehmens Informationen finden lassen, die in dieser Form eigentlich nicht für bestimmte Mitarbeiterebenen bestimmt sind oder von einem im Büro weilenden Besucher der Firma beim Blick auf den Bildschirm gelesen werden.

BvD: Fallen lauern also überall. Ein externer Dokumentenlogistiker ist also zunächst vor allem auch Berater?
Gerhard Friederici: Das stimmt. Auch wenn das Informationsmanagement inhouse dargestellt wird, gibt es altbewährte Abläufe zu analysieren und viele wichtige Fragen zu beantworten, um den gesamten Lebenszyklus eines Schriftstücks oder eines Datenträgers auf den Prüfstand zu stellen. Lagert eine verantwortliche Stelle diese Aufgaben teilweise oder komplett aus, kommen noch ein paar zusätzliche Fragen für die Prozessgestaltung hinzu, aber im Gegenzug profitiert die Behörde oder das Unternehmen von der Kompetenz und dem darin enthalten Erfahrungsschatz eines spezialisierten Dienstleisters. Im Idealfall werden somit Ressourcen bei Personal und Räumlichkeiten für die Kernaufgaben des Auftraggebers frei. Vor allem aber wird die Sicherheit der Daten, deren Schutz in der Wissensgesellschaft eine hohe Priorität besitzt, garantiert.

„Die neue DIN-Norm 66399 zur Gewährleistung einer datenschutzkonformen Akten- und Dokumentenvernichtung ist ein gutes Beispiel, wie sich Prozesse im Dialog mit allen Beteiligten standardisieren und somit professionalisieren lassen“, sagt Gerhard Friederici von Rhenus, hier auf einer gemeinsamen Veranstaltung von Rhenus und dem BvD. (Foto: Michael Braun)

BvD: Wie erkenne ich einen zuverlässigen Dienstleister?
Gerhard Friederici: Das Schiller-Wort „Drum prüfe, wer sich ewig bindet“ gilt aus meiner Sicht auch hier. Eben weil dem Schutz der eigenen Daten ein so hoher Wert beigemessen wird, muss genau geprüft werden, mit welchem Anbieter zusammengearbeitet wird. Die Zertifikate, die das dafür notwendige Vertrauen herstellen sollen, basieren in unserer Branche noch zu selten auf allgemein anerkannten Kriterien. Das erschwert die Auswahl des Dienstleisters. Deshalb ist in der Presse auch immer wieder von Datenpannen zu lesen, obwohl ein Dokumentenlogistiker beauftragt war. Die neue DIN-Norm 66399 zur Gewährleistung einer datenschutzkonformen Akten- und Dokumentenvernichtung gibt hier ein gutes Beispiel, wie sich Prozesse im Dialog mit allen Beteiligten standardisieren und somit professionalisieren lassen. Diesen Weg werden wir kontinuierlich weitergehen müssen, um Informationen vor einem unberechtigten Zugriff zu schützen.

Die EU-DSGVO aus Sicht französischer Behörden

CNIL sieht französische Bedenken als weitesgehend beseitigt an

Der französische Rechtsrahmen zum Schutz personenbezogener Daten besteht vor allem aus dem Gesetz vom 6. Januar 1978 („Loi Informatique et Libertés")[1], einem der ältesten Datenschutzgesetze Europas. In Frankreich wird traditionell von einem sehr hohen Schutz des Betroffenen ausgegangen. Dabei war Frankreich schon immer einer der Staaten, die sich an der Entwicklung und Diskussion rund um diesen Themenbereich sowohl innerhalb der Europäischen Union als auch auf der internationalen Bühne auffallend beteiligten. Die Grundsätze des französischen Gesetzes vom 6. Januar 1978 stellten zusammen mit den deutschen Datenschutzgrundsätzen die Ecksteine der Europäischen Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten dar. Am 25. Januar 2012 stellte die Europäische Kommission den Entwurf einer Datenschutzgrundverordnung vor,[2] welche die Richtlinie von 1995 modernisieren soll. Der Entwurf wurde seit der Veröffentlichung sehr ausführlich von den französischen Behörden sowie Gesetzgebern thematisiert und untersucht.

I. Pluspunkte für die Stärkung der Betroffenenrechte, aber mit Vorbehalt

Beide Kammern des französischen Parlaments, Abgeordnete und Senatoren, nahmen zu dem Entwurf der Europäischen Kommission Stellung und scheinen der gleichen Meinung zu sein, was die Vorteile des europäischen Entwurfes, aber auch dessen Lücken betrifft. Tatsächlich weicht die Ansicht des französischen Senats[3] nicht sonderlich von der zuvor veröffentlichen Stellungnahme der Nationalversammlung ab.[4] Nach Meinung des Senats war die Novellierung des europäischen Rechtsrahmens für den Datenschutz auf Grundlage der Richtlinie 95/46/EG längst überfällig, zumal die fast 20-jährige Richtlinie aufgrund der technologischen Entwicklungen und der Entstehung neuer Anwendungen obsolet geworden ist. Mit der von der Kommission nun angestrebten Modernisierung verfolgt der EU-Gesetzgeber das Ziel, Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern.[5] Die französischen Gesetzgeber begrüßen ihrerseits vor allem die durch die Reform angestrebte Förderung bestehender Rechte sowie Einführung neuer Rechte für die Bürger.

Recht auf Vergessenwerden (Art. 15 des Entwurfes)

Das „Recht auf Vergessenwerden" oder „droit à l´oubli" ist ein Konzept, das die französischen Juristen freuen dürfte. Als Richterrecht allgemein verbreitet im Strafrecht, dem Pressegesetz und dem Recht auf Privatsphäre, wurde es vom französischen Datenschutzjargon übernommen. Diese Erfindung des französischen Datenschutzes vermittelt in der Tat eine wichtige Botschaft - die der zeitlichen Begrenzung der Speicherdauer von Daten; was dem Einzelnen das legitime Recht auf „habeas data"[6] gewährleisten würde. Einer der größte Befürworter der Kodifizierung dieses Rechtes ist der Professor Jean Frayssinet[7], der der Meinung ist, „der Mensch solle nicht sein ganzes Leben lang von Daten gestört werden, die ohne seine Kenntnis gespeichert und verwendet werden." Jeder solle sein legitimes Recht auf Vergessenwerden genießen dürfen.

Gleichwohl die französischen Abgeordneten davon überzeugt sind, dass der massive Austausch personenbezogener Daten, die Internationalisierung des Handels, die Kommerzialisierung personenbezogener Daten, der Werbereiz persönliche Informationen, die neuen technologischen Möglichkeiten sowie die Verbesserung der Speicherkapazität von Daten in bisher unvorstellbarem Ausmaß so viele Elemente sind, die den Anspruch eines Rechts auf Vergessenwerden begründen, bleibt jedoch die Erkenntnis, dass die Umsetzung eines allgemeinen Rechts auf Vergessenheit möglicherweise nicht durchführbar ist. Sie schlagen zum Wohle des Re-

Autorin

Dr. Victorine Kossi
LL.M.Kundendatenschutz (CDK)
Konzerndatenschutz
DB Mobility Logistics AG

alismus vor, dieses Pflichtgebot in erster Linie nur auf soziale Netzwerke zu verlagern.

Befestigung des Grundsatzes der Einwilligung bei der Verwendung personenbezogener Daten (Art. 7 des Entwurfes)

Das Prinzip der expliziten Einwilligung im französischen Datenschutzgesetz nahm vor allem Bezug auf die Verarbeitung von sensiblen Daten.[8] Die französischen Behörden begrüßen nun, dass dieses Recht auf Einwilligung nach Artikel 7 Abs. 4 des Entwurfs für jede Datenverarbeitung unabhängig von der Art der Daten gilt, denn eine Einwilligung muss zukünftig„ explizit" gegeben werden und kann nicht mehr „angenommen" werden. Es ist ihrer Ansicht nach wichtig, dass eine stillschweigende oder passive Zustimmung nicht mehr als Grundlage für eine Datenverarbeitung dienen darf. Vielmehr würde eine Einwilligung eine aktive Herangehensweise der betroffenen Person voraussetzen.

In ihrer Auslegung dieser neuen Vorschrift gehen die Abgeordneten noch weiter und stellen fest, dass eine Einwilligung nur dann rechtmäßig ist, wenn die Verarbeitung personenbezogener Daten auf einer ausdrücklichen freien und informierten Zustimmung der betroffenen Person beruht. Die Person sollte eine echte Wahl haben. Diese Auslegung knüpft an das Konzept der Integrität der Einwilligung im französischen Zivilrecht an, wie es in Art. 1109 des französischen Bürgerlichen Gesetzbuchs vorgeschrieben ist.[9] Auch wenn die Einwilligung darin nicht positiv definiert wird, ist diese nach der von der Norm vorgesehenen Negativabgrenzung nur dann rechtsgültig, wenn sie keine Willensmängel aufweist.

Verpflichtung zur Datenübertragbarkeit (Art. 18 des Entwurfes)

Nach Auffassung französischer Datenschutzexperten ist das Ungleichgewicht zwischen Nutzern und Anbietern von Diensten wie Facebook in der fehlenden Datenübertragbarkeit begründet. Das Individuum verliert die Fähigkeit seine Rechte auszuüben, und insbesondere das Recht ohne Zwang auf einen Online-Service zu verzichten[10] oder den Dienstleister zu wechseln. Dies ist wahrscheinlich einer der Gründe, warum die französische Nationalversammlung der Meinung ist, dass die Datenportabilität das Recht der Betroffenen auf Zugang zu ihren eigenen Daten vereinfachen würde sowie auch die Weitergabe ihrer personenbezogenen Daten von einem Dienstleister zu einem anderen. Dieser Meinung ist auch Jeremie Zimmermann[11], der die Datenübertragbarkeit mit der Frage der Zugriffsrechte verbindet. Nach seiner Auffassung sollte dies bedacht werden, um den Anforderungen an Interoperabilität, Verwendung offener Formate und das Recht zur freien Wahl eines Formats für die Datenweitergabe einzubinden. Von nun an sollte die Datenportabilität dazu führen, um – wenn möglich auf europäischer Ebene – eine echte Pflicht zur Datenweitergabe von Bürgern durchzusetzen.[12] Die CNIL[13] ist der Auffassung, dass die Entwicklung eines Rechts auf Portabilität ein wesentliches Instrument für den Schutz personenbezogenen Daten sein wird.

II. Rechenschaftsprinzip: Mehr Verantwortung der für die Datenverarbeitung Verantwortlichen

Neben der Stärkung der Betroffenenrechte begrüßen die Franzosen die verstärkte Umsetzung des

Nach der Veröffentlichung des Berichtsentwurf von EU-Berichterstatter Jan Philipp Albrecht (Foto) stellte die CNIL klar, dass der Bericht ihrer Ansicht nach die Bedenken der Franzosen im Zusammenhang mit dem Verordnungsentwurf weitgehend beseitigt hat.
(Foto: Michael Braun)

Grundsatzes der Verantwortlichkeit beim Umgang mit personenbezogenen Daten.

Verpflichtung zur früheren Risikoerkennung und Folgenabschätzung (Art. 23, 33, 39 ff. des Entwurfes).

Unternehmen werden dem Entwurf der Verordnung nach bei der Datenverarbeitung stärker in Rechenschaft gezogen und insbesondere darauf verpflichtet, geeignete technische und organisatorische Maßnahmen schon bei der Planung und Konzeption von Projekten („privacy by design") einzubeziehen (Art. 23 des Entwurfes).

Ferner müssen sie risikoreiche Datenverarbeitungen auf ihre möglichen Auswirkunken zu untersuchen (sog. Datenschutz-Folgenabschätzung nach Art. 33 des Entwurfes) und sich bzw. ihre Produkte Zertifizierungsverfahren sowie Datenschutzsiegeln (Art. 39 des Entwurfes) unterwerfen.

Verschärfung der Sanktionen (Art. 79 des Entwurfes)

Darüber hinaus werden die verwaltungsrechtlichen Sanktionen der Aufsichtsbehörden verschärft und die Höhe der Bußgelder heraufgesetzt (Art. 79 des Entwurfes). Der erklärte Zweck dieser Änderungen ist, eine erheblich abschreckende Wirkung auszulösen und große Player wie Google, Facebook und Co. von Datenschutzverstößen abzubringen. Die bisher festgelegten Bußgelder scheinen Großunternehmen nicht erheblich irritiert zu haben. Dagegen sollte die Verhängung einer Geldbuße bis zur Höhe von 2% des weltweiten Umsatzes mehr als einen Großkonzern beim Umgang mit personenbezogenen Daten sorgfältiger werden lassen, wenn man bedenkt, wie viel Umsatz sie jährlich weltweit machen.[14] Ob die Aufsichtsbehörden diese Bußgelder jedoch tatsächlich in der Praxis umsetzen werden, wird man sehen. Denn während das französische Gesetz derzeit ein Bußgeld von bis zu 300.000 Euro zulässt[15], beläuft sich das bislang höchste von der CNIL verhängte Bußgeld auf (nur) 100.000 Euro. Dieses war 2011 gegen Google verhängt worden, nachdem das Unternehmen bei seinem Dienst Google Street View unter anderem auch unzulässigerweise WLAN-Daten erhoben und gespeichert hatte.

Data breach Notification (Art. 31 des Entwurfes)

Auch bei der in Art. 31 des Entwurfs normierten Pflicht, betroffene Personen über eine Datenpanne bzw. einen unberechtigten Zugang zu deren Daten zu informieren, handelt es sich nach Auffassung des französischen Nationalversammlung um einen sehr bedeutenden Schritt. Wenn auch Frankreich bisher anders als einige seiner europäischen Nachbarn wie Deutschland oder Großbritannien nur wenig unter Skandalen um den Verlust oder die unrechtmäßige Weitergabe von persönlichen Daten zu leiden hatte, ist das Niveau des Datenschutzes bzw. der Datensicherheit in Frankreich aus Sicht der CNIL weiterhin unzureichend und eine Reform der Regelungen zur Data Breach Notification begrüßenswert. Allerdings herrscht in Frankreich bislang große Unsicherheit darüber, welche Anbieter der Meldepflicht unterfallen, da das französische Datenschutzgesetz den Adressaten nicht näher definiert.

Neben der Unsicherheit in Hinblick auf den Verpflichteten der Norm ist auch unklar, wann eine Meldung im Sinne von Artikel 34 des französischen Datenschutzgesetzes noch „unverzüglich" ist. Auch hier fehlt es an einer gesetzlichen Vorgabe, stattdessen liegt die Frage nach der Unverzüglichkeit im Ermessen der CNIL. Diese Rechtsunsicherheiten wären mit der neuen EU-DSGVO beseitigt, denn Art. 31 des Entwurfes beschränkt die Informationspflicht nicht auf eine bestimmte Kategorie von wirtschaftlichen Akteuren und führt konkrete zeitliche Vorgaben bei der Meldepflicht ein.

Entlastung bei Meldepflichten

Auch der Abbau von Bürokratie ist für Frankreich, ein Land, in dem fast alles zentralisiert ist, ein großes Anliegen. Die CNIL hat bereits dafür gesorgt, dass bestimmte Datenverarbeitungsvorgänge von der Meldepflicht befreit werden bzw. diese erleichtert wird. So werden Meldepflichtverfahren bei gewöhnlichen Datenverarbeitungsverfahren privilegiert um vereinfachten Regeln unterworfen werden zu können. Für die gewöhnlichen Datenverarbeitungen im öffentlichen sowie im privaten Bereich, die offensichtlich weder Privatsphäre noch Freiheiten beeinträchtigen, stellt die CNIL Standardnormen fest und veröffentlicht diese.[16] Der Verantwortliche muss bei derartigen Verfahren lediglich anhand eines vorbereiteten Formulars erklären, dass die geplante Datenverarbeitung einer Standardnorm ‚xy' entspricht. Ein Erfolg, weil die aktuelle Zahl dieser Art von Meldungen 80% der Anzahl aller Meldungen übersteigt. Der Senat be-

grüßt daher die Vereinfachung und Modernisierung der deklaratorischen Formalitäten, da dies das große Ziel des Bürokratieabbaus vorantreibt und folglich auch eine Entlastung der Verantwortlichen bei den Meldepflichten und eine Reduzierung von Kosten mit sich bringt.

In Kürze

Die französischen Senatoren und Abgeordneten sind den europäischen Projekten zur Modernisierung des Rechtsrahmens zum Schutz personenbezogener Daten insgesamt sehr positiv begegnet. Auch wenn die herrschende Meinung in Frankreich ist, dass die Verordnung längst überfällig war und sie gegenüber ihrer Vorgängerin auf jeden Fall Fortschritte bringt, sind der Senat und die Nationalversammlung kritisch was einige aus ihrer Sicht wichtige Punkte betrifft. Sie fordern z.B. einen Verzicht auf die One Stop Shop-Lösung, um die Rechte der Bürger nicht zu schwächen. Sie wünschen außerdem eine größere Freiheit der Datenschutzbehörden bei Untersuchung sowie Kontrolle und dass sie am Prozess der Ausarbeitung normativer Vorhaben beteiligt werden.

Nach der Veröffentlichung des Berichtsentwurf von Jan Philipp Albrecht, dem Berichterstatter des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Nationalversammlung[17], am 8. Januar 2013 äußerte sich die CNIL mit Genugtuung, da der Bericht ihrer Ansicht nach die Bedenken der Franzosen im Zusammenhang mit dem Verordnungsentwurf weitgehend beseitigt habe. Sollten die Vorschläge aus dem Berichtsentwurf von der Europäischen Nationalversammlung verabschiedet und mit ihrem aktuellen Gehalt von der Kommission akzeptiert werden, wären sowohl der französische Senat, das Abgeordnetenhaus, die CNIL als auch die Justizbehörde damit höchst zufrieden. Desto erstaunlicher ist es festzustellen, dass trotz der insgesamt positiven Sicht von großen Ländern wie Frankreich und Deutschland immer noch keine Einigung in Sicht ist. Die Verzögerungen liegen vermutlich darin, dass die positive Kritik überwiegend von Behörden/Regierungen kommt. Betroffen von der Verordnung ist allerdings vor allem die Privatwirtschaft, die bei der Gesetzgebung dem Anschein nach vergessen wurde und die jetzt versucht, mit viel Lobbyarbeit diesen Entwurf scheitern zu lassen.

Textverweise

1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
2) Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig, abrufbar unter http://ec.europa.eu/justice/data- protection/document/review2012/com_2012_11_de.pdf.
3) Auf die Initiative von Simon Sutour, dem Vorsitzenden des Ausschusses für europäische Angelegenheiten nahm der Senat am 6. März 2012 den Entwurf einer europäischen Entschließung zur EU-DS-GVO an. Abrufbar unter http://www.senat.fr/dossier-legislatif/ppr12-343.html.
4) Hierzu Proposition de résolution européenne sur la proposition de règlement relatif à la protection des personnes physiques à l´égard du traitement des données à caractère personnel et à la libre circulation des données. Abrufbar unter http://www.assemblee-nationale.fr/13/rapports/r4325.asp
5) S. die Pressemitteilung der Europäischen Kommission vom 25. Januar 2012 zur Veröffentlichung des Entwurfs der DS-GVO, abrufbar unter http://europa.eu/rapid/press-release_IP-12-46_de.htm.
6) Frayssinet, Informatique, fichiers et libertés, P1992, S. 74.
7) Jean Frayssinet ist Professor an der Rechtsfakultät der Universität Aix Marseille III und Datenschutz-Spezialist.
8) Artikel 8 II.1 französisches Datenschutzgesetzes
9) In Artikel 1109 Code Civil heißt es, dass „keine gültige Zustimmung erteilt wurde, wenn diese versehentlich gewährt, gewaltsam abgenötigt oder durch arglistige Täuschung erreicht wurde".
10) So Daniel Le Metayer, Research Director bei INRI, einer öffentlichen Forschungseinrichtung, die sich der digitalen Wissenschaft und Technologie widmet.
11) Jeremie Zimmermann ist Mitbegründer von „La Quadrature du Net", eine Hilfsorganisation für die Rechte und Freiheiten der Bürger im Internet. Diese Organisation fordert eine treue Anpassung der französischen und europäischen Gesetzgebung an die Werte, die die Entwicklung des Internets geleitet hat – insbesondere den freien Verkehr von Wissen.
12) CNIL, Cahier Innovation et Prospective n°1 : Le futur de la vie privée vu par 42 experts
13) Die CNIL, Commission nationale informatique et libertés, ist die französische Datenschutzaufsichtbehörde mit Sitz in Paris, Webauftritt unter http://www.cnil.fr/.
14) Allein Facebook macht jährlich weltweit Umsätze in Höhe von hunderten Millionen US-Dollar, vgl. die Statistik von Statista zum weltweiten Umsatz Facebooks zwischen dem 1. Quartal 2010 und dem 4. Quartal 2012, abrufbar unter http://de.statista.com/statistik/daten/studie/237434/umfrage/umsatz-von-facebook-weltweit-quartalszahlen/ (abrufbar nur nach Anmeldung bei Statista).
15) Délibération n°2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc., abrufbar unter http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf. Eine englische Version der Pressemitteilung ist abrufbar unter http://www.cnil.fr/linstitution/actualite/article/article/google-street-view-la-cnil-prononce-une-amende-de-100-000-euros/.
16) http://www.cnil.fr/documentation/deliberations/normes-simplifiees/
17) Entwurf eines Berichtes über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 –2012/0011(COD)) Ausschuss für bürgerliche Freiheiten, Justiz und Inneres Berichterstatter: Jan Philipp Albrecht

Jugendschutz-Programme – für ein sicheres Surfen?

Software ersetzt keinesfalls die Medienerziehung in der Familie – Anregungen kommen aus der Praxiserfahrung der BvD-Initiative

Aus der Arbeit der Initiative „Datenschutz geht zur Schule“ des BvD entwickeln sich vielfältige Fragestellungen, aber auch Kontakte im Umfeld der medienpädagogischen Kompetenz. Der folgende Beitrag widmet sich daher einem Thema, das nicht nur Erziehungsberechtigte betrifft, sondern auch verantwortliche Stellen nach dem BDSG wie Jugendeinrichtungen. Aus Sicht eines Jugendamtes werden Hintergründe und Möglichkeiten des Jugendschutzes im Internet dargestellt, ergänzt um Hinweise aus Datenschutzsicht.

Das Internet bringt neben der Vielzahl an Information- und Interaktionsangeboten auch eine Menge an entwicklungsbeeinträchtigenden und jugendgefährdenden Inhalten mit sich. Mit einem Mausklick kann ein Kind gewollt oder ungewollt auf einer Seite mit harter Pornografie oder extremen Gewaltdarstellungen landen.

Der Gesetzgeber versucht diese Gefährdungen durch gesetzliche Bestimmungen für Kinder und Jugendliche zu minimieren. Im Sinne des Jugendschutzgesetzes und Jugendmedienschutz-Staatsvertrages dürfen Internetinhalte, die geeignet sind die Entwicklung von Kindern und Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen oder zu gefährden, nicht für ihre Altersstufe freigegeben werden (vergl. §§ 4 und 5 Jugendmedienschutz-Staatsvertrag, im folgenden JMStV).

Die Kommission für Jugendmedienschutz der Landesmedienanstalten (KJM, siehe auch www.kjm-online.de) legte daher im Mai 2012 fest (FAQ „Anerkannte Jugendschutzprogramme, zu finden unter http://kjm-online.de/files/pdf1/_FAQ_Inhalteanbieter.pdf), dass jeder Anbieter von Internetinhalten deshalb dafür Sorge tragen muss, dass Kinder und Jugendliche auf entwicklungsbeeinträchtigende Angebote üblicherweise nicht zugreifen können. Zu diesem Zweck kann er auch auf anerkannte Jugendschutzprogramme zurückgreifen und seine Inhalte dafür programmieren. Er kommt damit seiner gesetzlichen Verantwortung gegenüber Kindern und Jugendlichen nach und kann von der Aufsicht nicht mehr belangt werden. Programmieren bedeutet nach der KJM, dass der Anbieter seine entwicklungsbeeinträchtigenden Inhalte korrekt kennzeichnen (= „labeln“) muss. Korrektes „Labeling“ bedeutet, dass Anbieter ihre Inhalte der richtigen Altersklasse zuordnen und mit einem technischen Standard (age-de.xml) so auszeichnen, dass die Klassifizierung von anerkannten Jugendschutzprogrammen ausgelesen und richtig interpretiert werden kann.

Jugendgefährdende Inhalte wie z.B. pornografische Seiten dürfen in Deutschland nach wie vor nur über „geschlossene Benutzergruppen“ verbreitet werden (§ 4 Abs. 1 Punkt 10 iVm § 4 Abs. 2 JMStV).

Jugendschutzprogramme ≠ Filterprogramme

Die KJM definiert, dass Jugendschutzprogramme gemäß § 11 JMStV damit ausschließlich ein Instrument der Privilegierung von Inhalte-Anbietern darstellen. Sie sind deshalb nicht mit Jugendschutzfiltern zu verwechseln, wie sie von Filterherstellern entwickelt und als Schutzmaßnahme für Familien, Schulen, Internet-Cafes oder Jugendeinrichtungen angeboten werden (http://kjm-online.de/de/pub/jugendschutz_in_telemedien/jugendschutzprogramme.cfm)).

Dennoch kommen die anerkannten Jugendschutzprogramme letztendlich natürlich auch Erziehungsberechtigten zu Gute, da diese eine qualitative, leicht handhabbare und kostenlose Beschränkung von problematischen Internetinhalten für Familien-PCs ermöglichen. Die davon zu unterscheidenden

Jugendschutzfilter funktionieren für den privaten Gebrauch deshalb u.U. ähnlich gut wie derzeit anerkannte Programme, nur erfüllen Anbieter von Internetinhalten damit nicht die gesetzlichen Bedingungen.

Öffentliche Einrichtungen und Betriebe

Laut den obersten Landesjugendbehörden unterliegen auch öffentlich zugängliche Einrichtungen wie Schulen, Einrichtungen der Kinder- und Jugendhilfe, Bibliotheken, Bürgerhäuser, Stellen der Bundesagentur für Arbeit, Einrichtungen der Aus-, Fort- und Weiterbildung in gemeinnütziger oder öffentlicher Trägerschaft oder vergleichbare Einrichtungen/Träger sowie deren Vernetzung bzw. deren Anschluss an das Internet grundsätzlich den Beschränkungen des Jugendschutzgesetzes (JuSchG) sowie des JMStV. Das heißt, sie dürfen keine entwicklungsbeeinträchtigende oder jugendgefährdende Online-Inhalte für Minderjährige zugänglich machen.

Nach der „Rechtsauffassung der Obersten Landesjugendbehörden (OLJB) zur jugendschutzrechtlichen Einordnung von Computerräumen mit und ohne Internetzugang in Jugendeinrichtungen oder Schulen, sowie zur Veranstaltung sog. LAN-Parties durch Schulen“ aus den Jahr 2005 kann dies durch die Beachtung folgender Maßgaben umgesetzt werden:

- die Installierung einer geeigneten Filtersoftware
- gelegentliche, stichprobenartige Kontrolle der aufgerufenen Seiten durch Kontroll- oder Servicepersonal
- gelegentliche Kontrolle des Internetprotokolls
- einsehbare Aufstellung der Bildschirme

Die Datenschutzbeauftragten, die hierzu beraten, werden dabei beachten müssen, inwieweit durch Filtersoftware die Lauffähigkeit weiterer erforderlicher Software beeinträchtigt werden kann. Die Kontrollen der aufgerufenen Seiten und die Kontrolle des Internetprotokolls unterliegen wiederum den Rahmenbedingungen der datenschutzrechtlichen Regelungen, wie z. B. § 32 BDSG, sofern es sich um minderjährige Auszubildende handelt. Am rechtlich und technisch unproblematischsten ist von den vorgeschlagenen Maßnahmen die einsehbare Aufstellung der Bildschirme umzusetzen, wie es sich in der Regal auch bei öffentlichen Internetcafés beobachten lässt.

Anerkannte Jugendschutzprogramme

Seit 2012 wurden nun zwei dieser Jugendschutzprogramme unter Auflagen von der zuständigen Behörde (Kommission für Jugendmedienschutz – KJM) anerkannt. Es handelt sich dabei um ein Programm des JusProg e.V. (http://www.jugendschutzprogramm.de), sowie um ein Programm der deutschen Telekom (kostenlos, nur für Telekom Kunden erhältlich). Inhaltlich funktionieren beide Programme sehr ähnlich. Die Anerkennung erfolgte für beide zunächst unter Auflagen, da die Funktionalität noch nicht entsprechend der Vorgaben durch die KJM umfassend gegeben ist.

JusProg im Praxistest

Durch die kommunale Stelle für Jugendmedienschutz in Nürnberg wurde das Programm JusProg auf Praxistauglichkeit getestet, beispielsweise für den Einsatz in Einrichtungen der offenen Kinder- und Jugendarbeit. Der kostenlose Download und die Installation erfolgten unkompliziert. Auf manchen Rechnern musste, je nach System, ein ebenfalls kostenloses Zusatzprogramm (NET 4.0) installiert werden, welches mit einer Verlinkung angegeben wurde.

Zu Beginn ließen sich verschiedene Voreinstellungen vornehmen, wie die Angabe eines Elternpasswortes (zum aktivieren/deaktivieren), oder die Einstellung von verschiedenen Benutzern mit den zugehörigen freigegebenen Altersstufen (ab 0, 6, 12, 16, 18 Jahren).

Außerdem war es möglich, über eine manuelle Einstellung der black- und whitelist bestimmte Seiten zusätzlich zu blocken, bzw. bewusst zuzulassen. Die Festlegung von bestimmten Surfzeiten ist der kostenpflichtigen Premiumversion vorbehalten. Bei Fragen hilft ein umfassender Frage- und Antwortkatalog auf der Webseite des Herstellers (FAQ = Frequently Asked Questions).

Im Test wurden verschiedene harmlose Seiten, aber auch Seiten mit Gewalt- und pornografischen Darstellungen getestet. Pornografische Inhalte wurden insgesamt gut gefiltert, jedoch

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

Aus der Tätigkeit der BvD-Initiative „Datenschutz geht zur Schule" – hier eine Unterrichtseinheit mit Dozent Frank Spaeing in Berlin – ergeben sich vielfältige, hilfreiche Fragestellungen hinsichtlich des Jugendschutzes.

konnte man bei gezielter Suche auch Seiten mit entsprechenden Inhalten aufrufen (auch über kyrillische oder asiatische Schriftzeichen). Eine 100%ige Filterung war deshalb in diesem Bereich nicht möglich. Inhalte mit Gewaltdarstellungen und Rassismus wurden insgesamt nur unzureichend herausgefiltert. Gerade über das Video-Portal „youtube" konnten unzählige entwicklungsbeeinträchtigende Filme aufgerufen werden.

Social Communities wie Facebook wurden durch die Filterung teilweise sehr langsam. Die „google-Bildersuche", die gerade bei Kindern sehr beliebt ist, blockierte auch harmloses Bildmaterial. Kostenlose Browserspiele konnten teilweise auch nach Freigabe über die whitelist nicht gestartet werden, da die Startseiten auf weitere Unterseiten zugreifen und diese nicht explizit über die whitelist freigegeben waren. Hier sollte man laut Anbieter im „Quellcode" der Startseite nachsehen, welche Seiten beim Starten mit aufgerufen werden und diese ergänzend in die whitelist aufnehmen.

Ob dies weniger technisch versierten Eltern zuzutrauen ist, mag auch trotz Unterstützung durch die oben genannten FAQ bezweifelt werden.

Insgesamt betrachtet griff bei harmlosen Inhalten das sogenannte „Overblocking", also auch das Herausfiltern von harmlosen Seiten für Kinder. Im Bereich Pornografie funktionierte das Programm gut bis sehr gut, auch wenn es bei gezielter Suche umgangen werden konnte. Bei den „user generated content", also den von den Nutzern ins Netz gestellten Inhalten, tat sich das Programm teilweise schwer, bzw. funktionierte unzureichend, gerade im Bezug auf Gewalt und Rassismus. Außerdem sind die Programme derzeit noch nicht auf mobilen Endgeräten wie Smartphones installierbar. Da Netzinhalte jedoch zunehmend von Kindern und Jugendlichen mobil aufgerufen werden, ist dies dringend zu empfehlen.

Die genannten Kritikpunkte hat auch die KJM als weitere Erwartung an die Programmhersteller herausgegeben (http://kjm-online.de/files/pdf1/Anlage_zu_PM_4_2013__Jugendschutzprogramme.pdf). Jugendschutzprogramme bieten nach dem aktuellen Stand die Möglichkeit, Internetinhalte für Kinder und Jugendliche zu begrenzen. Allerdings stellen sie nur eine flankierende Maßnahme dar und ersetzen keinesfalls die Medienerziehung in der Familie. Erziehungsberechtigte und die Verantwortlichen von Einrichtungen sollten zeitig klare Surfregeln vereinbaren und überprüfen und als Ansprechpartner bei auftauchenden Problemen zur Verfügung stehen. Auch müssen diese Personen bereit sein, nach der Installation Zeit für die Modifizierung des Filters zu investieren.

Weitere Informationen hierzu sind bei www.kjm-online verfügbar. Die Initiative Klicksafe (http://www.klicksafe.de) bietet auch einen Leitfaden für den Jugendschutzfilter JusProg zum kostenlosen Download an.

Autor

Michael Posset
Fachkraft für Jugendmedienschutz beim Amt für Kinder und Jugendliche und Familien
Infos: www.jugendmedienschutz.nuernberg.de

Rudi Kramer
Rechtsanwalt, BvD Vorstand

Die Stiftung Datenschutz als Partner in Bildungsfragen

Jugend als Hauptzielgruppe der neu gegründeten Einrichtung

Das Wissen über Möglichkeiten zum aktiven Schutz der eigenen Daten bedarf ständiger Auffrischung und Ausweitung. Angesichts der rasant fortschreitenden technischen Möglichkeiten zum Sammeln und Verknüpfen von personenbezogenen Daten kommt den Prinzipien von Selbstdatenschutz und Datensparsamkeit wachsende Bedeutung zu. Die Förderung der Bildung in diesem Bereich ist daher eine der zentralen Aufgaben der STIFTUNG DATENSCHUTZ. Sie wird auf Bundesebene eine Informationsplattform bieten, mit der die bereits vorhandenen Initiativen der Landesbehörden und weiterer Stellen ergänzt werden sollen.

Die Bundesrepublik beschritt in diesem Jahr mit der Gründung einer unabhängigen Stiftung einen neuen Weg im Bereich der Datenschutzpolitik. Die Stiftung nach bürgerlichem Recht ist auf Dauer angelegt und kann ungeachtet tagespolitischer Diskussionen langfristige Lösungswege verfolgen. Die anerkannte Gemeinnützigkeit verbietet dabei ihr eine einseitige Vorgehensweise und erfordert es, die Belange des Datenschutzes zum allgemeinen Wohl zu verfolgen.

Der Informationsbedarf wächst: Nur wer die Möglichkeiten zum Schutz der Privatsphäre kennt, kann sie auch nutzen. Und nur wer weiß, welche Folgen ein leichtfertiger Umgang mit persönlichen Informationen haben kann, wird sich stets Gedanken machen, bevor er eine Information, die seinen privaten Bereich betrifft, versendet oder ins Netz stellt. Ein wesentlicher Schlüssel um Datenmissbrauch zu vermeiden liegt deshalb in der generellen Sensibilisierung der sogenannten Datensubjekte, der Personen also, deren Privatsphäre es zu schützen gilt. Bürgerinnen und Bürger als Träger des Grundrechts der informationellen Selbstbestimmung sollen ermutigt und befähigt werden, dieses Recht souverän auszuüben und über eine Preisgabe von Teilen ihrer Privatsphäre zu jeder Zeit informiert und frei zu entscheiden.

Die Möglichkeit einer Beeinträchtigung der eigenen Persönlichkeitsrechte wurde bei vielen Internetnutzern bislang oft ausgeklammert – sei es, weil kein Szenario einer Bedrohung bekannt ist („wer sollte denn außer meinen Freunden schon wissen wollen, wo ich abends unterwegs bin ?“), sei es, weil die Wahrscheinlichkeit einer Gefährdung zu gering erscheint oder keine Fälle aus dem Freundeskreis bekannt sind. In den letzten Monaten ist bei manchen diese Sorglosigkeit einem gewissen Erschrecken gewichen angesichts der nun bekannten riesigen Überwachungsmöglichkeiten ausländischer Nachrichtendienste. Teilweise wird hierauf mit Internet-Abstinenz reagiert, teilweise herrscht Fatalismus und meistens Ratlosigkeit. In jedem Fall besteht ein großer Bedarf an Informationen zum Selbstschutz.

Jugend als Hauptzielgruppe: Bildung zum Schutz der Privatsphäre kann nicht früh genug ansetzen. Deshalb wird die STIFTUNG DATENSCHUTZ unter anderem ein Bildungsprogramm speziell für Interneteinsteiger konzipieren. Verbraucherbildung soll schon bei den ganz jungen Teilnehmern am öffentlichen Leben im Internet beginnen, denn aus zu geringer technischer Kenntnis oder infolge zu geringen Weitblickes begangene frühe Fehler lassen sich später oft nur schwer wieder „einfangen“ – und einen digitalen Radiergummi gibt es in der Praxis noch nicht.

Bereits im Alter zwischen 6 und 9 Jahren finden heute erste spielerische Begegnungen mit dem Internet statt, teilweise auch schon mit Netzwerken wie facebook. Diese jüngsten Teilnehmer an den Kommunikationsprozessen in Datennetzen und Netzwerken haben mangels (schlechter) Erfahrungen oft nur wenig Risikobewusstsein. Ihnen wurde Wissen über mögliche Gefahrenquellen für die Privatsphäre vielfach nicht vermittelt – teilweise, weil dies als noch nicht altersgerechtes Thema angesehen wird, teilweise schlicht aufgrund fehlender personeller oder zeitlicher Ressourcen. Aufklärung über Technikfolgen darf aber auch bei Kindern nicht nur zufällig oder anlassbezogen erfolgen. Wissen um Selbstdatenschutz sollte vermittelt werden, bevor es zu schlechten Erfahrungen kommt.

Unser Ziel wird es daher sein, den jungen Schülerinnen und Schülern auf spielerische Weise Inhalt und den Wert ihrer Privatsphäre vor Augen zu führen und ihnen erste

Kenntnisse für deren Schutz zu vermitteln. Das Aktionsprogramm soll praktisches Wissen zum Schutz der persönlichen Daten nahebringen. Sinnvolle Handlungsweisen sollen erklärt und empfohlen werden, ohne zu bevormunden. Es geht nicht darum, die „Datenfahrschüler" von ihrem Einstieg in den Verkehrsraum Internet abzuschrecken oder zu verunsichern. Ihnen sollen vielmehr Möglichkeiten zur sicheren Nutzung des Netzes aufgezeigt werden. Der Spaß soll dabei nicht auf der Strecke bleiben.

Info

Weitere Informationen unter:
www.stiftungdatenschutz.org

Angesichts voller Lehrpläne und immer weniger Schuljahren werden sich derartige Konzepte zunächst vor allem auf Projekttage und Projektwochen als mögliche Umsetzungszeiträume konzentrieren müssen. Später soll auf eine Integration des Bildungskonzepts in ein mögliches übergreifendes Fach zur Verbraucheraufklärung hingewirkt werden.

Als Vermittler vor Ort kommen für ein solches Aufklärungsprogramm neben technisch versierten Lehrerinnen und Lehrern vor allem externe Fachleute in Frage. Diese können datenschutzbezogene Inhalte aufgrund ihrer technischen Vorkenntnisse glaubhaft vermitteln und erregen als Experten von außen und besondere Gäste regelmäßig mehr Unterrichtsaufmerksamkeit als es die gewohnten Lehrpersonen können. Zu denken ist hier neben Datenschutzbeauftragten und (pädagogisch geschulten) Informatikern eventuell auch an Studierende aus dem IT-Sektor.

Programme für alle Altersgruppen: Zielgruppe von Aufklärungs- und Bildungsprogrammen im Bereich des Datenschutzes werden darüber hinaus auch ältere, IT-fern und unvernetzt aufgewachsene Bevölkerungsgruppen sein. Diese treten dem Internet und seinen Anwendungen oft mit großer grundsätzlicher Skepsis gegenüber und nutzen daher viele technische Dienste gar nicht oder sehr zurückhaltend. Gerade auch Bedenken hinsichtlich des Datenschutzes spielen dabei eine große Rolle, weswegen Aufklärung auch in diesem Bereich lohnt.

Angebote zur Kooperation: In Bezug auf die Kompetenzen der Länder in Bildungsfragen ist die Abgrenzung klar. Die STIFTUNG DATENSCHUTZ des Bundes wird in keinerlei Zuständigkeiten einzugreifen versuchen. Vielmehr wird sie den Landesschulverwaltungen und den Schulen vor Ort Angebote zur Zusammenarbeit machen. Die unterbreiteten Konzepte setzen die Bildungseinrichtungen bei erkanntem Bedarf nach landesrechtlichen Vorgaben und ihren eigenen Vorstellungen in der Praxis um. Bei der Bewältigung von personellen Engpässen in der Vermittlung datenschutzbezogener Inhalte wird die Stiftung auszuhelfen versuchen, sobald ihre Struktur gewachsen sein wird und dies zulässt. Auch mit den Beauftragten der Länder für den Datenschutz wird die Stiftung sich abstimmen und über Kooperationen sprechen. Im föderalen Verbund, so sind wir überzeugt, wird sich das Niveau an Datenschutzkenntnissen in allen Altersgruppen heben lassen. Die Befähigung zum Selbstdatenschutz und das generelle Bewusstsein im Umgang mit der eigenen Privatsphäre werden so befördert.

Im privaten Bereich der Datenschutzaufklärung kommt natürlich vor allem der BvD als Kooperationspartner in Frage. Vor allem die mit der Initiative „Datenschutz geht zu Schule" seit Jahren aufgebaute praktische Erfahrung und Bildungskompetenz kann guten Rat für ergänzende Bildungskonzepte geben.

Ausblick Datenschutzgütesiegel: Neben der Entwicklung von Bildungskonzepten liegt eine weitere Hauptaufgabe der STIFTUNG DATENSCHUTZ in der Vereinheitlichung im Zertifizierungsbereich. Die Entwicklung eines einheitlichen und bekannten Datenschutzgütesiegels soll dazu beitragen, Datenschutzanstrengungen vom vermeintlichen Wettbewerbshemmnis zum Wettbewerbsvorteil zu machen. Mit der Stiftungsarbeit sollen die bestehenden Ansätze und der in der privaten und staatlichen Zertifizierungspraxis seit Jahren vorhandene Sachverstand zusammengebracht werden. Der STIFTUNG DATENSCHUTZ wird dabei eine Scharnierfunktion zukommen, um die erprobten Systeme mit den verschiedenen Akteuren wie dem Unabhängigen Datenschutzzentrum Schleswig-Holstein oder privaten Prüforganisationen wie dem TÜV weiterzuentwickeln. Durch einheitliche Standards soll mehr Wiedererkennbarkeit und mehr Nachfrage nach dem allgemeinen Siegel erreicht werden.

Die betrieblichen Datenschutzbeauftragten sind in den Auditierungsprozess eingebunden; ihre Kenntnisse sind für die am Beginn der Auditierung regelmäßig durchzuführende Bestandsaufnahme unverzichtbar. Sie stellen die ersten Ansprechpartner für die externen unabhängigen Auditoren dar.

Die Zertifizierungsvereinheitlichung und die Aufklärungsbemühungen ergänzen sich als Stiftungsaufgaben gegenseitig. Während Bildungsprogramme allgemein die datenbezogene Sensibilität steigern sollen, haben die Gütezeichen die Aufgabe, den sensibilisierten Datensubjekten die Auswahl ihrer Vertragspartner zu erleichtern.

Autor

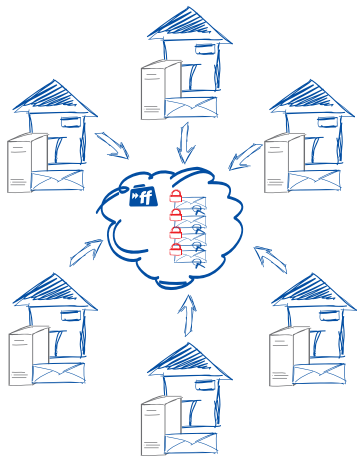
(Foto: Lorenz Becker)

RA Frederick Richter LL.M.
Präsident der
Stiftung Datenschutz
Karl-Rothe-Straße 10-14
04105 Leipzig
E-Mail: Richter@
stiftungdatenschutz.org

D-BUSINESS® FolderFlex

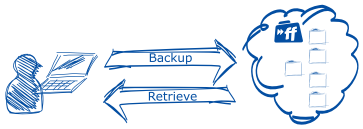
Infrastruktur: D-BUSINESS® FolderFlex ist ein Tool zum sicheren Datenaustauch großer Dateien zwischen Geschäftspartnern. D-BUSINESS® FolderFlex sichert Daten und hält diese für deren Austausch, Verbreitung oder Zugriff eines berechtigten Dritten online vor und kann an bestehende Strukturen, Compliancevorgaben, bestehende Unternehmens-CIs und Workflowprozesse angepasst werden. Dabei kann D-BUSINESS® FolderFlex als OnlineDienst gemietet oder als Appliance zum internen Unternehmenseinsatz erworben werden.

Sicherer Datenspeicher
D-BUSINESS® FolderFlex ist jederzeit verfügbar und kann nicht verlegt werden. Ihre Mitarbeiter verlieren nie wieder einen USB-Stick, denn sie benötigen keinen. Der Datenaustausch mit beispielsweise Kunden und Lieferanten wird somit zum Kinderspiel. Zusätzlich wird jeder Empfang, jede Bearbeitung und jeder Versand einer Datei manipulationsfrei im Logbuch gespeichert.



Datenaustausch - schnell und sicher!

- 10GB Daten an 100 Personen mit einem Klick!
- Unter Berücksichtigung sämtlicher Datenschutzrichtlinien
- Mit Protokolierung
- Mit Abrufrückmeldung



Vergessen Sie CD‘s und DVD‘s ...
... D-BUSINESS® FolderFlex macht es möglich!

Scenario 1 - Sicherer Dateiupload via D-BUSINESS® FolderFlex Empfangsbox
Mit der passwortgeschützten Empfangsbox kann Ihnen jede berechtigte Person qualifiziert Dateien anliefern. Über definierbare Fragen im Uploadprozeß wird die Dateiablage zusätzlich gesteuert und vereinfacht. Optional werden alle Gruppenmitglieder über die Datenanlieferung per Mail informiert.

Scenario 2 - Sicherer Dateidownload via D-BUSINESS® FolderFlex Direct Download
Für den Empfang einer mit FolderFlex versendeten Datei benötigt der Empfänger lediglich einen Onlinezugang. Der interne Absender wählt die zu sendenden Dateien über die DirectLink-Funktion und gibt die E-Mail-Adresse des Empfängers ein. Der Empfänger erhält eine E-Mail mit einem passwortgeschützten Link, direkt auf die ihm zugeteilten Dateien die er nach Passworteingabe sofort herunterladen kann. Der gesamte Vorgang wird protokolliert.

Highlights

- **Direkt starten!** FolderFlex ist eine webbasierende Anwendung die in jedem Internetbrowser läuft. Es ist keine Installation notwendig.
- **Vertrauliche Daten.** Innerhalb einer Firma können Gruppen definiert werden, die nur für dafür registrierte Benutzer sichtbar sind.
- **Dropbox und Webshare.** Versand und Empfang beliebig großer Datenmengen für nichtregistrierte Benutzer.
- **Datengröße.** 200 Gigabyte pro Datei sind möglich.
- **BDSG Konform.** Alle Datenbewegungen erfüllen die Anforderungen und Bestimmungen des Europäischen Datenschutzgesetzes.

Nutzen

- Ihre Mitarbeiter können jederzeit auf benötigte Daten zugreifen.
- Ihre Geschäftspartner können auf zugewiesene Ordner und Dateien zugreifen, Daten anliefern und ggf. in Gruppen integriert werden.
- Sie können jederzeit nachweisen Wer, mit Wem, Wann, Welche Daten ausgetauscht hat.

Datenschutzprüfung bei Einsatz von Adobe Analytics

Konkrete Erfahrungen bei einer „kleinen Großprüfung“

Im Jahr 2012 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bei ca. 13.000 Webseiten bayerischer Anbieter den datenschutzgerechten Einsatz von Google Analytics geprüft. Bereits damals hat das BayLDA darauf hingewiesen, dass nicht nur das Produkt eines Anbieters, sondern mindestens noch ein weiteres Produkt einer Prüfung unterzogen werden soll. Bei der automatisiert durchgeführten Prüfung von Google Analytics hatte sich ergeben, dass etwa 2.500 Webseiten das Produkt nicht datenschutzkonform einsetzen, so dass diese individuell angeschrieben und angehalten werden mussten, die entsprechenden datenschutzrechtlichen Vorgaben einzuhalten. Die Durchführung dieser Großprüfung, insbesondere die Beantwortung telefonischer und auch per E-Mail eingegangener Rückfragen zeigte dem BayLDA mit seinen 16 Mitarbeiterinnen und Mitarbeitern zeitweise die Grenze der Belastbarkeit auf. Als Folge dieser Prüfung wurde dann innerhalb des BayLDA ein Konzept entwickelt, wie weitere kleinere oder größere Prüfungen durchgeführt werden sollen, um ressourcenschonend auch den sonstigen Dienstbetrieb aufrechterhalten zu können. Am Beispiel der „kleinen Großprüfung“ des datenschutzgerechten Einsatzes von Adobe Analytics soll der Prüfungsablauf im Folgenden näher dargestellt werden.

Vorbereitung der Prüfung: Dieser Prüfung gingen intensive und konstruktive Gespräche mit der Firma Adobe voraus, die dazu führten, dass die Voreinstellung der Gültigkeitsdauer der Tracking-Cookies von 60 auf 24 Monate reduziert wird, die Geolokalisierung der Webseitenbesucher bei entsprechender serverseitiger Einstellung nur noch an Hand einer durch Kappung des letzten Oktetts anonymisierten IP-Adresse erfolgt und daneben die IP-Adresse - ebenfalls bei entsprechender serverseitiger Einstellung - vor Auswertung der Webseitenaktivitäten durch eine generische IP-Adresse ersetzt wird. Die Notwendigkeit einer zweimaligen Anonymisierung besteht, da die Geolokalisierung mittels der IP-Adresse bei Adobe Analytics zunächst getrennt von der Auswertung stattfindet und erst die gewonnene Information über den geographischen Ort in die Statistik einfließt. Ohne die zweimalige Anonymisierung läge jeweils eine Verwendung der IP-Adresse vor, für die keine Rechtsgrundlagen ersichtlich wären. Sowohl Kürzung und Überschreibung der IP-Adresse als auch die Speicherung der Nutzungsdaten finden grundsätzlich in der Europäischen Union statt. In den Gesprächen wurde Einvernehmen darüber erzielt, welche datenschutzrechtlichen Anforderungen an den Einsatz dieses Produktes zu stellen sind und was gegebenenfalls von Nutzern der Produkte gemacht werden muss. Das BayLDA hat sich bei diesen Gesprächen an den Vorgaben des Düsseldorfer Kreises, die er in seinem Beschluss vom 26./27. November 2009 zum Ausdruck gebracht hat (http://www.lda.bayern.de/onlinepruefung/Beschluss_Reichweitenmessung.pdf), und auch an den Hinweisen für Webseitenbetreiber, die der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit mit der Firma Google für den Einsatz von Google Analytics vereinbart hat (http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_01.pdf), orientiert. Diese Verständigung hatte für die Nutzer des Produkts den Vorteil, dass sie unabhängig davon, ob sie sich an den Anbieter ihres Produkts oder das BayLDA gewandt haben, eine gleichlautende Antwort bekommen (sollten).

Mit einem selbst entwickelten Prüfprogramm wurde eine große Anzahl von bayerischen Webseiten zunächst daraufhin überprüft, ob dort Adobe Analytics im Einsatz ist. Soweit dies der Fall war, wurden die entsprechenden Anschriften der Webseitenanbieter erfasst und in einem manuellen Verfahren der Einsatz von Adobe Analytics nochmals überprüft.

In einem weiteren Schritt wurde überlegt, welche Fragen von den Benutzern kommen könnten und

dazu entsprechende Informationen auf die Homepage des BayLDA gestellt (siehe: http://www.lda.bayern.de/onlinepruefung/adobeanalytics.html). Um sicher zu gehen, dass Rückfragen zur Prüfung zeitnah beantwortet werden können, wurde dann der Termin für das Absenden der entsprechenden Schreiben mit den geplanten Urlaubszeiten der betroffenen Mitarbeiterinnen und Mitarbeiter abgestimmt.

Ziel der Prüfung: Ziel dieser Prüfung war grundsätzlich, dem gesetzlichen Auftrag der Datenschutzaufsichtsbehörde Rechnung zu tragen. Nachdem es möglicherweise immer noch Unternehmen in Bayern geben könnte, die von der Existenz und der Aufgabenstellung des BayLDA nichts wissen, trägt eine derartige Prüfung insoweit auch zur Horizonterweiterung bei. Ein weiterer Nebeneffekt ist die Erhöhung des gefühlten Risikos „erwischt zu werden". Und nicht zuletzt zeigen die Rückmeldungen aus dem Kreis der Datenschutzbeauftragten, dass eine derartige Prüfung als Rückenstärkung für betriebliche Datenschutzbeauftragte wirkt, da deren Hinwirken auf die Unternehmensleitung dadurch Unterstützung erhält. Alle diese Bemühungen tragen schließlich im Ergebnis dazu bei, dass dem Schutz der Betroffenen bei der Wahrung ihres Rechts auf informationelle Selbstbestimmung jedenfalls ein Stück mehr Rechnung getragen wird.

Ablauf der Prüfung: Mit Schreiben vom 14. Juni 2013 hat das BayLDA 44 Unternehmen angeschrieben, die nach einer automatisierten Auswertung von nunmehr ca. 15.000 Webseiten bayerischer Anbieter Adobe Analytics einsetzen. In diesem Schreiben wurde auf die folgenden Anforderungen des datenschutzgerechten Einsatzes dieser Trackingsoftware hingewiesen:

• Vertrag zur Auftragsdatenverarbeitung: Der Nutzer muss einen Vertrag zur Auftragsdatenverarbeitung schriftlich abschließen. Dieser Vertrag zur Auftragsdatenverarbeitung wird auf Anfrage von Adobe bereitgestellt.
• Angebot einer Widerspruchsmöglichkeit: Der Nutzer muss dem Besucher seiner Webseite eine effektive Widerspruchsmöglichkeit gegen das Setzen von Tracking-Cookies durch Adobe Analytics anbieten. Dabei ist insbesondere darauf zu achten, dass die Widerspruchsmöglichkeit bei allen Browsern wahrgenommen werden kann. Dies gilt besonders für Browser von Smartphones, z.B. bei einem Webangebot, das speziell für die mobile

Die „kleine Großprüfung" der BayLDA profitierte vom neu entwickelten Verfahren.

Nutzung ausgelegt ist.

• Angepasste Datenschutzerklärung: Der Nutzer muss in seiner Datenschutzerklärung den Besucher seiner Webseite über die Erhebung und Verwendung personenbezogener Daten im Rahmen von Adobe Analytics aufklären und auf die Widerspruchsmöglichkeit gegen die Erfassung durch Adobe Analytics hinweisen.

• Serverseite Einstellungen: Serverseitig muss eingestellt werden, dass die IP-Adresse des Besuchers der Webseite vor der jeweiligen Verarbeitung insbesondere für die Geolokalisierung und die Reichweitenmessung unabhängig voneinander anonymisiert wird, d.h. die IP-Adresse vor der Geolokalisierung um das letzte Oktett gekürzt und die verwendete IP-Adresse durch eine generische IP-Adresse ersetzt werden.

• Laufzeit der Cookies: Die Laufzeit der Cookies ist auf das notwendige Mindestmaß zu begrenzen. Als Obergrenze wird eine Dauer von 24 Monaten angesehen.

Diesem Schreiben war ein bis zum 30. Juli 2013 zurückzuschickender Fragebogen beigefügt, in dem u. a. darüber Auskunft gegeben werden sollte, ob das Produkt noch eingesetzt wird, ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen wurde, die Webseite eine Datenschutzerklärung enthält, eine Widerspruchsmöglichkeit gegen das Setzen von Tracking-Cookies gegeben ist, die vollständigen IP-Adressen der Webseitenbesucher vor der Geolokalisierung um das letzte Oktett gekürzt und vor der Auswertung der Webseitenaktivitäten durch eine generische IP-Adresse ersetzt werden und welche Laufzeit der Tracking-Cookie hat.

Innerhalb der gesetzten Frist haben 40 Unternehmen geantwortet, drei Unternehmen wurde auf entsprechenden Antrag eine Fristverlängerung eingeräumt, ein Unternehmen hat sich gar nicht geäußert und damit gemäß § 43 Abs. 1 Nr. 1 BDSG den Tatbestand einer Ordnungswidrigkeit erfüllt. In der Folgezeit hat sich auch das letzte Unternehmen gemeldet und eine - noch nicht abgelaufene - Fristverlängerung eingeräumt bekommen. Die drei Unternehmen, denen vorher schon eine Fristverlängerung eingeräumt worden war, haben ihre Stellungnahme abgegeben, so dass heute die Antworten von 43 Unternehmen vorliegen. Anders als bei der Prüfaktion bei Google Analytics zeigte sich bei dieser Prüfung, dass das kostenpflichtige Programm Adobe Analytics in der Regel von größeren Firmen eingesetzt wurde, die über fachlich geschultes Personal verfügen, so dass sich die Rückfragen zur Implementierung der Vorgaben für einen beanstandungsfeien Einsatz von Adobe Analytics und damit der Arbeitsaufwand für die Datenschutzaufsichtsbehörde sehr in Grenzen hielt.

Auswertung der Rückmeldungen: Aus den 43 vorliegenden Antworten der Unternehmen ergibt sich, dass sechs das Produkt nicht mehr einsetzen. Überraschend und ein Stück erschreckend war schließlich, dass von den verbliebenen 37 Unternehmen lediglich fünf Unternehmen zum Zeitpunkt der Prüfung im Juni 2013 über einen abgeschlossenen Vertrag zur Auftragsdatenverarbeitung mit der Firma Adobe verfügten und 32 Unternehmen diesen erst im Zuge des Prüfverfahrens abgeschlossen haben. Auch dieses Verhalten (praktizierte Auftragsdatenverarbeitung ohne erforderlichen Vertrag) erfüllt den Tatbestand einer Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 2b BDSG. Entsprechende Bußgeldverfahren wurden vom BayLDA nicht eingeleitet, da Ziel dieser Prüfung primär die datenschutzkonforme Nutzung von Adobe Analytics war. Bei Vorliegen dieser Voraussetzungen ist aber für die Zukunft vorgesehen, bei entsprechenden Feststellungen durchaus ein Bußgeldverfahren einzuleiten.

Zwar stellt Adobe die Software zur Reichweitenmessung her, die datenschutzrechtliche Verantwortlichkeit liegt allerdings bei den Nutzern der Software. Die Webseitenbetreiber beauftragen Adobe damit, die Daten ihrer Webseitenbesucher zu erheben, für den Zweck der Reichweitenmessung zu verwenden und Auswertungen und Statistiken der Webseitenaktivitäten zu erstellen. Adobe ist somit als weisungsgebundene Stelle Auftragsdatenverarbeiter i.S.d. § 11 BDSG und in diesem Rahmen grundsätzlich weder Adressat von aufsichtsrechtlichen Maßnahmen noch von Bußgeldern. Das BayLDA geht aber davon aus, dass die Firma Adobe ihren Vertragspartnern - jedenfalls in Zukunft - im Zweifel von sich aus entsprechende Verträge vorlegen wird, um ihre Auftraggeber vor einem Bußgeldverfahren zu bewahren.

Die anderen Anforderungen bezüglich Datenschutzerklärung, Widerspruchsmöglichkeit und Anonymisierung der IP-Adressen wurden durchgehend

Autor

Thomas Kranig
Präsident, Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss), 91522 Ansbach
Tel: 0981 . 53-1302
Fax: 0981 . 53-5300
E-Mail: thomas.kranig@lda.bayern.de
http://www.lda.bayern.de

als erfüllt bestätigt und waren, soweit sich dies in Stichproben nachprüfen ließ, auch umgesetzt. Ebenso wurde die Lebensdauer der Tracking-Cookies auf maximal 24 Monate begrenzt.

Fazit: Als Fazit dieser „kleinen Großprüfung" lässt sich zunächst festhalten, dass eine strukturierte Planung des Prüfablaufs die Prüfung deutlich erleichtert (eigentlich eine Binsenwahrheit) und im Interesse aller Beteiligten sicherstellt, dass die Prüfung zeitnah abgeschlossen werden kann. Die Tatsache, dass zum Zeitpunkt der Prüfung vorbehaltlich der noch ausstehenden Antwort, jedenfalls 32 von 37 Unternehmen, die geantwortet haben, d.h. mehr als 85%, Adobe Analytics ohne den erforderlichen Vertrag zur Auftragsdatenverarbeitung eingesetzt haben, zeigt erhebliche Mängel bei der Beachtung datenschutzrechtlicher Vorschriften, selbst wenn es sich - jedenfalls in Bezug auf bußgeldrechtliche Gewichtung in § 43 Abs. 1 und Abs. 2 BDSG - insoweit „nur" um formelle und nicht um materielle datenschutzrechtliche Verstöße handelt. Allerdings hat der Vertrag zur Auftragsdatenverarbeitung gem. § 11 BDSG konstitutive Wirkung, so dass ein Datenumgang personenbezogener Daten ohne Abschluss eines solchen Vertrages nicht im Sinne einer Auftragsdatenverarbeitung privilegiert ist. Es stellt sich in diesem Zusammenhang auch die Frage nach der Fachkunde und Zuverlässigkeit der Datenschutzbeauftragten, nach denen in diesem Prüfverfahren nicht gefragt wurde, die es aber wegen der Größe der Unternehmen in der Regel in den geprüften Unternehmen geben müsste. Das BayLDA nimmt das Ergebnis dieser Prüfung zum Anlass, zeitnah vergleichbare Prüfungen unter Einbeziehung von Fragen bezüglich der betrieblichen Datenschutzbeauftragten durchzuführen, zumindest in exemplarischen Fällen Bußgelder festzusetzen und diese Tatsache - unter Wahrung der Vertraulichkeit bezüglich des konkret betroffenen Unternehmens - eventuell auch mittels entsprechender Pressemitteilungen publik zu machen.

- 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

Mindestanforderungen an das Berufsbild des Compliance-Officer

20 Themenfelder beschreiben die Rechte und Pflichten

Die Anzahl compliance-relevanter Regularien und Sachverhalte ist in der jüngeren Vergangenheit enorm angestiegen. Dieser Trend hält weiter an. Presseberichten kann man klar entnehmen, dass Compliance-Vorfälle in den letzten Jahren ebenfalls stark zugenommen haben. Dies betrifft nicht nur einzelne Industriesäulen, sondern ist eine branchenübergreifende Entwicklung, sei es in der Bank- und Finanzdienstleistungsindustrie, der Versicherungsindustrie oder der produzierenden bzw. der Dienstleistungsindustrie. Die Auswirkungen auf die Tätigkeit eines Compliance-Officer sind heute noch nicht abzusehen.

Bekanntlich gibt es erhebliche Überschneidungen zwischen den Tätigkeitsfeldern von Compliance-Verantwortlichen und betrieblichen Datenschutzbeauftragten. Denn Compliance funktioniert erfahrungsgemäß nicht ohne effektive Kontrollen. Und solche Kontrollen setzen in aller Regel das Erheben und Verwenden personenbezogener Daten voraus. Gerade bei Compliance-Kontrollen oder internen Ermittlungen ist daher der Interessenkonflikt zwischen der Überprüfung normgerechten Verhaltens und den Persönlichkeitsrechten der Betroffenen offensichtlich. Besonders klar zeigt dies etwa ein Urteil des Bundesgerichtshofs in Strafsachen, in dem die Richter Privatermittler wegen unzulässiger Kontrollmaßnahmen zu Haftstrafen nach § 44 BDSG verurteilten. Gerade dieser Fall zeigt klar, dass sich Compliance-Verantwortliche auch im Datenschutz auskennen müssen und umgekehrt.

BDCO stellt Anforderungen an das Berufsbild auf

Das Aufgabenumfeld eines Compliance-Officer nimmt immer mehr zu. Haftungsfragen in Bezug auf die eigene Arbeit stellen sich immer häufiger. Es wird somit immer wichtiger, das Aufgabenfeld eines Compliance-Officer klar abzugrenzen und zu definieren.

Der BDCO Bundesverband Deutscher Compliance-Officer hat hierzu Mindestanforderungen an das Berufsbild eines Compliance-Officer veröffentlicht.

Best Practices definieren und mit Aufsichtsbehörden abstimmen

Diese Mindestanforderungen haben eine ähnliche Stoßrichtung wie das berufliche Leitbild des Datenschutzbeauftragten des Bundesverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.. Allerdings sind die Vorgaben des BvD auf den Datenschutzbeauftragten begrenzt. Die Mindestanforderungen an das Berufsbild des Compliance-Officer des BDCO gelten für alle Compliance Officer im weiteren Sinne. Dies gilt branchenübergreifend und für alle Industriesäulen.

Auf einem Treffen des Frankfurter Compliance-Kreises sprachen sich zahlreiche namhafte Compliance-Officer für die Gründung eines Verbands zur Vertretung von Compliance-Verantwortlichen aus. Auch Vertreter von Aufsichtsbehörden unterstützen das Vorhaben. Aus dem Expertengremium zum Erfahrungsaustausch und zur Information über Compliance-Themen ist der BDCO Bundesverband Deutscher Compliance-Officer hervorgegangen.

Der BDCO will Unternehmen und Compliance-Officern dabei helfen, eine herausfordernde und komplexe Aufgabe effektiv zu bewältigen. Das unternehmensspezifische Berufsbild und die Aufgaben eines Compliance-Officer sollen präzisiert werden. Zudem sollen Best Practices definiert werden und diese mit den Aufsichtsbehörden abgestimmt werden. Stellungnahmen zu Gesetzesvorhaben werden eingebracht, Praxistipps, Checklisten und Handlungsempfehlungen werden abgegeben.

Die Tätigkeit des BDCO ist nicht auf einzelne Branchen beschränkt. Sie sollen einen umfassenden und branchenübergreifenden Austausch der Erfahrungen zwischen den unterschiedlichen Industrie-

und Dienstleistungszweigen ermöglichen, um so gemeinsame Lösungsansätze und entsprechende Standards zu entwickeln. Der BDCO wird den Informationen zu Compliance-Themen zwischen Unternehmen, Mitgliedern, relevanten Behörden, Politik und anderen Verbänden transportieren. Hierzu erarbeitet der BDCO gemeinsame Compliance-Standards und stimmt diese ab. Er fördert die Prävention von Straftaten und Ordnungswidrigkeiten durch die Schaffung wirksamer Compliance-Strukturen. Der Verband ist keine Alternative zu bestehenden Branchenverbänden, sondern arbeitet bei Compliance-Themen eng mit diesen zusammen. Die weiteren Ziele des BDCO sind die nähere Bestimmung und professionale Sicherung des Berufsbilds, aber auch die Vertretung der Interessen von Compliance-Officern.

Mindestanforderungen in 20 Themenfelder gegliedert

Der BDCO gibt Stellungnahmen zu Rechtssitzungsinitiativen und anderen Compliance-relevanten Vorhaben ab. Der Verband bietet Handlungsempfehlungen für den Umgang mit komplexen regulatorischen Anforderungen in vielen Branchen. Zudem zeigt der BDCO praxisgerechte Lösungen für Zielkonflikte, zwischen Compliance-Anforderungen und andern rechtlichen Vorgaben auf. Neben mit Compliance-Themen beruflich befassten Personen können auch solche Unternehmen dem BDCO beitreten, die Compliance fördern oder sich über dieses Thema umfassend und zeitnah informieren wollen.

Das BDCO Positionspapier „Berufsbild des Compliance-Officers – Mindestanforderungen zum Inhalt, Entwicklung und Ausbildung“ ist das Erste seiner Art. Diese Mindestanforderungen und Leitlinien wurden im Arbeitskreis „Berufsbild des Compliance- Officer“ des BDCO erarbeitet. Sie dienen als Grundlage für die Entwicklung und Formulierung branchenübergreifender Best Practice, und zwar nicht nur für den jeweils für die Compliance-Funktion Verantwortlichen und registrierten Chief Compliance-Officer bzw. Compliance-Beauftragten, sondern auch für alle Mitarbeiter einer Compliance-Funktion. Besonderheiten können sich aus der Größe und Branche des jeweiligen Unternehmens sowie aus dessen spezifischem Risikoprofil ergeben.

Die Mindestanforderungen an das Berufsbild des Compliance-Officers des BDCO sind in 20 Themenfelder aufgegliedert. Die Themenfelder ent-

Der BDCO e.V. sieht sich als Ergänzung zu den Angeboten des BvD e.V.

halten zentrale Aussagen, die das Tagesgeschäft aber auch die strategische Positionierung von Compliance-Funktionen bzw. Chief Compliance-Officer/Compliance-Beauftragter beinhalten. Hierzu gehören Aussagen zu Verantwortlichkeiten für die Compliance-Funktion, Stellung und Unabhängigkeit eines Chief Compliance-Officer/Compliance-Beauftragen, aber auch die Vermeidung von Interessenkonflikten bzw. das Schnittstellenmanagement zu anderen Einheiten im Unternehmen werden angesprochen.

Die Mindestanforderungen nehmen Bezug auf die Risikoevaluierungs- und Risikosteuerungsfunktion von Compliance. Auch die Beratungs-/Kontroll- und Berichtspflichten werden definiert. Dabei wird die für die Risikosteuerungs- und Risikoevaluierungsfunktion notwendige unternehmensspezifische Risikoanalyse relevanter Gefährdungspotentiale zugrunde gelegt.

Aus- und Weiterbildung ist ein wesentlicher Fokus

Einen weiteren wesentlichen Fokus bildet die Aus- und Fortbildung von Compliance-Officern. Dabei ist es wichtig, dass Compliance-Officer selbstverständlich einen Überblick über das regulatorische Umfeld für die unternehmensspezifischen Geschäftsfelder haben. Dies alleine genügt jedoch noch nicht, um die Compliance-Funktion erfolgreich ausfüllen zu können. Die Kompetenzen des Compliance-Officer müssen sich auch über das regulatorische hinaus auf die durch das Unternehmen entwickelten und vertriebenen spezifischen Produkte beziehen. Auch sollte ausreichende Kenntnis zu Einkaufs- und Vertriebsstrukturen bestehen. Ganz wesentlich ist es, dass ein Compliance-Officer die jeweiligen Prozesse im eigenen Unternehmen kennt, versteht und bewerten kann. Ohne vertiefte Kenntnis von den im eigenen Haus bestehenden unternehmensspezifischen Prozessen ist zunächst eine erfolgreiche Compliance-Arbeit gerade auf der Beratungs- und Kontrollschiene nicht möglich.

In vielen Industriesäulen konzentriert sich Compliance fast ausschließlich auf die Beratungsfunktion. Dies ist eindeutig zu wenig, auch wenn das Motto gilt: Wer besser berät, muss weniger kontrollieren. Auch die Einhaltung der regulatorischen Vorgaben und unternehmensspezifischen Compliance-Vorgaben ist sicherzustellen. Dies entspricht auch den Vorstellungen eines internen Kontrollsystems, das auf der ersten Stufe die Verantwortlichkeit bei den jeweiligen Fach- und Geschäftsbereichen sieht. In der zweiten Stufe ist Compliance für die Einhaltung dieser Prozesse zuständig. Die interne Revision als Teil der dritten Stufe kontrolliert und prüft in einer neutralen Funktion das Bestehen und Funktionieren des sog. internen Kontrollsystems auf der ersten und zweiten Ebene. Dies bedeutet, dass eine Compliance-Funktion zwingend aus Beratungs- und Kontrollfunktionen bestehen muss, was in einzelnen Industriesäulen teilweise noch nicht vorhanden ist. Auch die Vermittlung der Compliance-Kultur und des Risikobewusstseins des eigenen Unternehmens soll durch die Compliance-Funktion anhand von Schulungen und Trainings vermittelt werden. Dies ist ein wesentlicher Bestandteil der Compliance-Arbeit, was sich bspw. auch im IDW PS 980 als Compliance-Standard niedergeschlagen hat.

Zur Wahrung der Unabhängigkeit und zur Stärkung der Compliance-Funktion ist es zwingend notwendig, dass die Berichtslinie des Compliance-Beauftragten/Chief Compliance-Officer nicht nur an den Vorstand (und zwar direkt und nicht über andere Leiter von Geschäftsbereichen, in einzelnen Industriesäulen oft noch über den General Counsel) erfolgt, sondern dass über den Vorstand bzw. die Geschäftsleitung die Compliance-Berichterstattung auch an das Aufsichtsgremium erfolgt. Damit ist sichergestellt, dass Compliance-Vorgaben und deren Einhaltung auch durch das Aufsichtsgremium kontrolliert werden können. Dieser Ansatz entspricht dem modernen Corporate Governance Verständnis von Compliance-Strukturen.

Compliance-Officer haben Rechte in allen Unternehmensbereichen

Wesentlich ist auch, dass Compliance-Officer zur effektiven Aufgabenerfüllung jederzeitige Informations-, Auskunfts-, Teilnahme- und Zugriffs- sowie Zutrittsrechte in allen Unternehmensbereichen haben. Den Mitarbeitern der Compliance-Funktion ist Zugang zu allen relevanten Informationen zu gewähren. Damit verbunden ist eine Eingriffspflicht (Vetorecht) für den Chief Compliance-Officer/Compliance-Beauftragten bei Verstößen gegen Compliance-Regularien. Bloße Warnhinweise, wie sie bspw. ein Legal Counsel aussprechen kann,

sind dabei nicht ausreichend. Eine Selbstverständlichkeit sollte sein, dass ein Compliance-Officer moralisch und rechtlich integer ist und eine hohe Zuverlässigkeit aufweist.

Die Compliance-Funktion ist unter Wahrung der rechtlichen Vorgaben auslagerbar. Bei mittleren bis größeren Unternehmen gestaltet sich dies jedoch schwierig. Bei kleineren Unternehmen kann dies durchaus eine mögliche Lösung sein, um die Compliance-Funktion sicher zu stellen. Dabei kann zwischen Auslagerung einzelner Teilaspekte (Beratung, Monitoring, Schulung) oder auch der Auslagerung der gesamten Compliance-Funktion (inkl. des Chief Compliance-Officers/Compliance-Beauftragten) unterschieden werden. Je nach Größe, Branche und Risikograd des Unternehmens sind verschiedene Lösungen denkbar. Zu beachten ist allerdings stets, dass die Verantwortlichkeit des Chief Compliance-Officers/Compliance-Beauftragten nicht teilbar ist und darüber hinaus die ultimative Verantwortung für Compliance immer bei der jeweiligen Unternehmensleitung als Gesamtorgan verbleibt.

Haftungsfragen: Einbezug in die D&O Versicherung empfohlen

Die Mindestanforderungen an das Berufsbild des Compliance-Officers schließen ab mit den für den Chief Compliance-Officer/Compliance-Beauftragter relevanten Haftungsfragen. Der Einbezug des Chief Compliance-Officer/Compliance-Beauftragten in die D&O Versicherung (Directors and Officers Versicherung) wird empfohlen. Darüber hinaus soll über eine gesonderte Vermögensschadenshaftpflicht oder eine Haftungsfreistellung des Unternehmens zur Wahrung seiner Unabhängigkeit nachgedacht werden.

Zum weiteren Schutz des Chief Compliance-Officer/Compliance-Beauftragten kann dessen besondere Stellung und Funktion Besonderheiten beim Kündigungsschutz nahelegen. Im Bankenumfeld gibt es bspw. eine Mindestbestellfrist von 24 Monaten für einen Compliance-Beauftragten. In den dortigen MaComp Mindestanforderungen an die Compliance-Funktion der BaFin ist auch die Empfehlung ausgesprochen, eine 12-monatige Kündigungsfrist zu Lasten des Arbeitgebers zum erweiterten Schutz des Compliance-Beauftragten vorzusehen. Hier könnte man mit gutem Grund über einen ähnlichen Kündigungs- oder Abberufungsschutz wie den des betrieblichen Datenschutzbeauftragten nachdenken.

Die den Datenschutzbeauftragten sicherlich bekannten Regeln des beruflichen Leitbilds des Datenschutzbeauftragten haben eine ähnliche inhaltliche Ausprägung und Gliederung wie die Mindestanforderungen an das Berufsbild des Compliance-Officers des BDCO. Die Vorgaben des BvD gliedern sich insbesondere in:
1. die persönlichen fachlichen Voraussetzungen eines Datenschutzbeauftragten,
2. die Aufgabenleistung des Datenschutzbeauftragten und
3. die Anforderung an die Berufsausübung.

Es lässt sich feststellen, dass bei synoptischer Übersicht beider Regelungen beide Papiere sich dem gleichen Ziel von unterschiedlichen Stoßrichtungen aus nähern. Beide fokussieren auf die Beratungsüberwachungsfunktion der jeweiligen Compliance-Officer bzw. Datenschutzbeauftragten. Es wird auf die besondere Stellung der jeweiligen Funktion eingegangen und Schutzmechanismen für Datenschutzbeauftragte bzw. Compliance-Officer diskutiert. Wesentlich ist die Unabhängigkeit beider Funktionen sowie die persönlichen und fachlichen Voraussetzungen, um die jeweilige Funktion ausführen zu können. Auch die Ausrichtung auf eine Prozessorientierung bei den im jeweiligen Unternehmen vorhandenen unternehmensspezifischen Prozessen ist deutlich erkennbar. Ferner nehmen beide Papiere besonderen Bezug zur Haftungssituation von Compliance-Beauftragten/Chief Compliance-Officer bzw. Datenschutzbeauftragte.

Fazit ist, dass die Ansätze des BDCO und des BvD die gleiche Stoßrichtung haben und sich gegenseitig ergänzen. Beide definieren das Berufsbild des Datenschutzbeauftragten bzw. Chief Compliance-Officer/Compliance-Beauftragten in einer ähnlichen Weise. Damit wird das Berufsbild eines Compliance-Officer im weiteren Sinne immer klarer und trennschärfer. Auch nehmen beide keine Begrenzung auf einzelne Industriesäulen vor. Beide Verbände haben nun vorgelegt. Es gilt, klare Vorgaben für das Berufsbild weiter zu entwickeln und einen gemeinsamen Standard für Chief Compliance-Officer/Compliance-Beauftragte bzw. Datenschutzbeauftragte zu fördern.

Autoren

Hartmut Renz
„Vice President Compliance Capital Markets“
HELABA, Landesbank Hessen Thüringen, Girozentrale
MAIN TOWER, MT 041000, Neue Mainzer Str. 52-58, 60311 Frankfurt am Main
Tel: 069 . 9132-5395
Fax: 069 . 9132-2019
Fax: 069 . 9132-85395 (PC)
E-Mail Hartmut.Renz@helaba.de

Tim Wybitul
of Counsel in den Bereichen Arbeitsrecht, Datenschutz, Compliance und interne Ermittlungen, Head of Compliance & Investigations Frankfurt, Hogan Lovells International LLP
Untermainanlage 1, 60329 Frankfurt
Tel: 069 . 96236-0
Fax: 069 . 96236-100
E-Mail tim.wybitul@hoganlovells.com

BYOD – Bring Your Own „Disaster“

Fragen zur Nutzung von privaten Geräten von Mitarbeitern

Mobile Geräte befähigen einige Mitarbeiter unzweifelhaft ihre Zeit produktiver zu nutzen, um zum Beispiel während einer Reise zu arbeiten. Heute besitzen die meisten Menschen verschiedene mobile Geräte: Mobiltelefone, die an sich schon kleine Computer darstellen, Laptops, Netbooks und/oder Tablet-PCs, wobei die Grenzen zwischen den letzten drei nicht immer klar definiert sind.

Der Einsatz der nicht dem Unternehmen gehörenden Geräte zu Firmenzwecken bieten dem Unternehmen auch Vorteile:

- Niedrigere Kosten im Bereich der Investitionen für IT-Mittel
- Nutzer kennen sich mit ihren privaten Geräten meist sehr gut aus, da sie diese selbst eingerichtet haben
  -> Geringerer Support-Bedarf
  -> Geringerer Schulungs-Bedarf
  Daraus resultiert insgesamt eine höhere Produktivität für das Unternehmen.
- Es steigert die Attraktivität eines Arbeitgebers, wenn sich Angestellte ihr Arbeitsgerät selbst aussuchen können.

Die Geräte im Besitz der Mitarbeiterinnen und Mitarbeiter sind im Vergleich zu den firmeneigenen Rechnern häufig mit zusätzlicher Funktionalitäten ausgestattet, welche auf den firmeneigenen Geräten vermisst werden und die Nutzwert für den Mitarbeiter erhöhen. Der Einsatz der nicht dem Unternehmen gehörenden Geräte für die tägliche Arbeit im Unternehmen bietet auf den ersten Blick den Mitarbeitern wie auch dem Unternehmen nur Vorteile: die Idee des BYOD (= „bring your own device“) war geboren.

Der zweite Blick: Durch die Offenheit der Gerätewahl steigert sich automatisch die Heterogenität[1] der mobilen Betriebssystemlandschaft im Unternehmen, wodurch sich der Aufwand der Administration und der Gestaltung der Sicherheitsrichtlinien drastisch erhöht, da die jeweiligen Merkmale eines Betriebssystems bzw. teilweise des jeweiligen Gerätetyps mit seiner entsprechenden Betriebssystemmodifikation (Stichwort: Android-Betriebs-

Bring your own device: Wenn Mitarbeiterinnen und Mitarbeiter ihre eigenen Geräte beruflich nutzen, kann das zu verschiedenen Problemen führen.

system ≠ Android Betriebssystem) evaluiert und für das Sicherheitskonzept berücksichtigt werden müssen. Daneben gibt es noch diverse andere Überlegungen, welche die unzweifelhaft vorhandenen Vorteile des BYOD-Konzeptes relativieren:

- Wie sieht es hinsichtlich der Produktivität des Mitarbeiters bei Verlust oder Defekt des mobilen Gerätes aus?
  - Stellt das Unternehmen ein Ersatzgerät?
  - Schließt das Unternehmen für das Gerät der Mitarbeiterin / des Mitarbeiters einen Supportvertrag ab?
- Benötigt das Unternehmen ggf. mehrere Remote Access Lösungen für die vielen verschiedenen Geräte?
- Wie schütze ich mein Unternehmensnetzwerk davor, dass von den privaten Geräten keine schädliche Software ins Unternehmen transportiert wird?

Weiterhin müssen verschiedene gesetzliche Regelungen betrachtet werden, insbesondere natürlich auch die bestehenden Datenschutzgesetze.

Unternehmen muss Herr der Daten bleiben

Werden Daten außerhalb der Verfügungsgewalt des Unternehmens gelagert, so dass das Unternehmen nicht mehr als „Herr der Daten" gelten kann, müssen die Daten letztlich als an einen Dritten übermittelt gelten. D.h. hier ist eine Einverständniserklärung der jeweils Betroffenen notwendig. Unabhängig vom Verwaltungsaufwand für das Unternehmen, der notwendig ist, um von allen Betroffenen ein Einverständnis einzuholen: wenn ein Betroffener sein Einverständnis nicht erteilt, muss dies in den IT-Systemen vermerkt werden und technisch verhindert werden, dass mit privaten Endgeräten auf die Daten zugegriffen werden kann, wohl aber mit dienstlichen Geräten.

Es muss also eine Liste geführt werden, mit denen eindeutig der Status „privat" bzw. „dienstlich" bestimmt werden kann und es müssen entsprechende Filterregeln in allen IT-Systemen implementiert werden. Zum heutigen Zeitpunkt ist dies so gut wie unmöglich abzubilden. Zudem ist das Unternehmen entsprechend §§17 und 18 UWG zum Schutz von Betriebs- und Geschäftsgeheimnisse verpflichtet, was ebenfalls eine direkte Weitergabe von derartigen Daten an Privatpersonen ausschließt.

Daher muss das Unternehmen auch beim Einsatz privater mobiler Endgeräte der „Herr der Daten" bleiben. Dies kann nur durch den Einsatz von Verschlüsselungssoftware erreicht werden, so dass auf den privaten mobilen Endgeräten Crypto-Container eingerichtet werden, in denen die Daten des Unternehmens gelagert werden. Idealerweise hat die Mitarbeiterin/der Mitarbeiter auf den Crypto-Container nur Zugriff, wenn das mobile Endgerät mit dem Unternehmensnetzwerk verbunden ist.

Bei Verlust des mobilen Endgerätes sind die dienstlichen Daten vor unbefugtem Zugriff geschützt. Ist das Unternehmen gezwungen, die dienstlichen Daten zu löschen, muss lediglich der Crypto-Container gelöscht werden; die privaten Daten der Mitarbeiterin/des Mitarbeiters bleiben unberührt.

Spezialgesetzliche Regelungen im Gesundheitswesen schreiben in einigen Bundesländern zudem vor, dass Daten grundsätzlich im Krankenhaus selbst verarbeitet werden müssen[2]. Auch der Landesbeauftragte für Datenschutz schreibt in seinem Tätigkeitsbericht, dass aus seiner Sicht der Einsatz privater Endgeräte nur ausnahmsweise in Betracht kommt, wenn ausschließlich Daten verarbeitet bzw. genutzt werden, die datenschutzrechtlich nicht als sensiblen anzusehen sind. In Fällen, wo nicht direkt auf dem Mobilgerät mit den Daten gearbeitet werden darf, kommen derzeit nur Terminal-Lösungen in Betracht, in denen die Verarbeitung im Krankenhaus erfolgt. Die zurzeit am häufigsten in Deutschland eingesetzte Lösung ist die von Citrix.

Rechtliche „Randbetrachtungen" bei BYOD

Bzgl. der Informationspflicht bei Datenpannen geht der Berliner Datenschutzbeauftragte davon aus, dass eine „Kenntniserlangung durch einen Dritten nicht positiv festgestellt" werden muss[3]. Desgleichen geht er davon aus, dass eine „Informationspflicht auch in Betracht kommt, wenn Laptops oder andere Datenträger an Orten verlorengehen, wo sie Dritten zugänglich sind und die Daten nicht verschlüsselt sind"[4]. Auch aus dieser Sicht ist ein Crypto-Container das Mittel der Wahl, denn ohne Verschlüsselung muss das Unternehmen bei Verlust des (privaten) mobilen Endgerätes seinen Informationspflichten nachkommen, d.h. ggf. eine Anzeige in überregionalen Tageszeitungen veröffentlichen. Neben dem Datenschutzrecht müssen

Textverweise

1) Stand 08.06.2012 bestand das Angebot der vier Carrier Telekom, Vodafone, O2 und E-Plus aus 168 verschiedenen Endgeräten; Quelle: Düll K. (2012) Bring Your Own Device (BYOD) - Wie viele Gerätetypen kommen denn da auf mich zu? [Online, überprüft 2013-10-06], verfügbar unter http://pretioso-blog.com/bring-your-own-device-byod-wieviele-geraetetypen-kommen-denn-da-auf-mich-zu/#.UlCC5FO1-Hs

2) Z.B.: Bremen (§10 BremKHDSG), Nordrhein Westfalen (§7 GDSG NW) oder auch Saarland (§13 SKHG)

3) 23. Tätigkeitsberichte des Landesbeauftragten für den Datenschutz Rheinland-Pfalz, S. 59. [Online, zitiert am 2013-05-14], verfügbar unter http://www.datenschutz.rlp.de/downloads/tb/tb23.pdf

4) Berliner Beauftragten für Datenschutz und Informationsfreiheit. (2011) FAQs zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG, S. 5,6 . [Online, zitiert am 2013-05-14], verfügbar unter http://www.datenschutz-berlin.de/attachments/809/535.4.7.pdf?1311923219

beim Einsatz von BYOD noch diverse andere rechtliche Fragestellungen betrachtet werden, wie beispielsweise:

- Arbeitsrecht
  - Kontrollmöglichkeit des Arbeitgebers bei privater Hardware entfällt („Computer-Grundrecht", BVerfG 27.02.2008)
  - TKG/TMG: Diensteanbieter -> begrenzter Zugriff auf Protokolldaten usw.
  - Kein Zugriff auf dienstl. E-Mails bei privaten Geräten
  - …
- Urheberrecht/Lizenzrecht
  - Installation von Software des Unternehmens auf privater Hardware vs. Urheberrecht (Evtl. Hinweis des Herstellers „Nutzung nur auf Rechnern, die im Eigentum des Lizenznehmers stehen"?)
  - Nutzung der privat gekauften Lizenzen für dienstliche Zwecke?
  - §99 UrhG: „Ist in einem Unternehmen von einem Arbeitnehmer oder Beauftragten ein nach diesem Gesetz geschütztes Recht widerrechtlich verletzt worden, hat der Verletzte die Ansprüche aus § 97 Abs. 1 und § 98 auch gegen den Inhaber des Unternehmens"
- Strafrecht; neben TKG, TMG und Datenschutz ist insbesondere §202a-c StGB zu betrachten
  - §202a StGB: Ausspähen von Daten
    - Keine Straftat, wenn private Daten beim Einsatz von BYOD nicht gesondert gesichert sind
  - §202b StGB: Abfangen von Daten
    - Keine Straftat, wenn Übermittlung über Unternehmenskommunikationsnetz erfolgt
  - §202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten
    - Keine Straftat, wenn der Täter nicht eine eigene oder fremde Straftat nach §202a oder §202b StGB unterstützen will
- Steuerrecht
  - Vergütungsanspruch des Mitarbeiters für die betriebliche Nutzung?
  - Geldwerter Vorteil
  - …
- Haftungsrecht
  - Verlust/Beschädigung Smartphone während Arbeit
  - Datenveränderung (§303a StGB), z.B. private Daten und Virenschutz des Unternehmens
  - …
- Vertragsrecht
  - Wer ist Vertragspartner für Wartung/Reparatur des Gerätes?
  - Wer ist verantwortlich für Updates?
  - …
- Compliance / Unternehmenssicherheit
  - Compliance := Auftraggeber hat insbesondere sicherzustellen, dass die
    - Integrität,
    - Vertraulichkeit,
    - Verfügbarkeit und
    - Zurechenbarkeit

    von Daten des Unternehmens bei unternehmenskritischen Prozessen und Anwendungen jederzeit sichergestellt ist
  - Arbeitgeber ist bei BYOD Auftragnehmer, wenn beispielsweise private Daten im Backup mitgesichert werden
  - …
- Geheimnisschutz
  - Schutz von Betriebs- und Geschäftsgeheimnisse (§§ 17, 18 UWG)
  - Verletzung von Privatgeheimnissen (§203 StGB)
  - …
- Betriebliche Nutzung privater Accounts
  - Social Network – wem gehört der Account?
  - …

Software zum Mobile Device Management (MDM)

Mobile Device Management (MDM) soll die zentrale Verwaltung der in einem Unternehmen eingesetzten mobilen Endgeräte ermöglichen. Die Anforderungen an eine MDM-Lösung sind:

- Sie ist kompatibel zu allen gängigen Mobile Plattformen und Anwendungen.
- Sie arbeitet in allen gängigen Mobilfunknetzen.
- Sie kann direkt „over the air" (OTA) implementiert werden unter Auswahl bestimmter Zielgeräte
- Hardware, Betriebssysteme, Konfiguration und Anwendungen können schnell und problemlos ausgeliefert werden.
- Mobile Geräte können nach Bedarf von Administratoren dem MDM-System hinzugefügt oder daraus entfernt werden, d.h. der Zugriff auf das Unternehmensnetzwerk und damit die Daten des Unternehmens darüber gesteuert werden.
- Die Integrität und Sicherheit der IT-Infrastruktur ist stets gewährleistet.
- Security Policies werden konsequent

Literatur

Arning M, Moos F, Becker M. (2012) Vertragliche Absicherung von Bring Your Own Device - Was in einer Nutzungsvereinbarung zu BYOD mindestens enthalten sein sollte. CR: 592-598

Bierekoven C. (2012) Bring your own Device: Schutz von Betriebs- und Geschäftsgeheimnissen - Zum Spannungsverhältnis zwischen dienstlicher Nutzung privater Mobilgeräte und Absicherung sensibler Unternehmensdaten. ITRB: 106ff

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2011) Überblickspapier Smartphones. [Online, zitiert am 2013-05-14]], verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2013) Überblickspapier IT-Consumerisation und BYOD. [Online, zitiert am 2013-05-14]], verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile

Conrad I, Schneider J. (2011) Einsatz von „privater IT" im Unternehmen - Kein privater USB-Stick, aber „Bring your own device" (BYOD)? ZD: 153ff

Deiters G. (2012) Betriebsvereinbarung Kommunikation - Beschäftigteninteressen und Compliance bei privater Nutzung von Kommunikationsmitteln im Unternehmen. ZD: 109ff

Göpfert B, Wilke E. (2012) Nutzung privater Smartphones für dienstliche Zwecke. NZA: 765ff

Hemker T. (2012) „Ich brauche das!" – Mobile Geräte im Unternehmenseinsatz - Übersicht über die Bedrohungslage und die Schutzmaßnahmen für die Verwendung geschäftlicher Daten auf (privaten) mobilen Geräten. DuD: 165-168

Herrnleben G. (2012) BYOD – die rechtlichen Fallstricke der Software-Lizenzierung für Unternehmen. MMR: 205ff

Hörl B. (2012) Bring your own Device: Nutzungsvereinbarung im Unternehmen - Mitarbeiter-PC-Programm als Steuerungsinstrument des Arbeitgebers. ITRB: 258ff

durchgesetzt.
- Der Anwender bekommt von der Existenz der Lösung so wenig wie möglich oder nötig mit.

Alle Anforderungen zugleich zu erfüllen schafft keine der auf dem Markt befindlichen Lösungen. Ein Unternehmen muss sich - wie bei der Anschaffung eines anderen Produktes auch – einen Kriterienkatalog erstellen, welche Anforderungen „muss"-Kriterien entsprechen, welche „kann"-Kriterien und welche „unerwünschtes feature"-Kriterien. Zu den Anforderungen können beispielsweise gehören

- Unterstütze (mobile) OS
  - Android
  - Blackberry
  - iOS
  - Symbian
  - Windows
  - …
- Security-Features
  - App-Installation (White-List, Black-List, …)
  - Authentifizierung-/Authorisierungs-Management
  - Jailbreak-Erkennung, rooten, …
  - …
- Systemintegration
  - AD/LDAP-Integration
  - App-Management
  - …

Danach müssen die eigenen Anforderungen mit den Möglichkeiten der angebotenen Produkte verglichen werden und idealerweise erfolgt dann eine Testinstallation der zwei, maximal drei besten Kandidaten. Ohne Anspruch auf Vollzähligkeit hier eine Liste mit Anbietern von MDM-Software:

- 7P Group (7P MDM)
  http://www.7p-group.com/portfolio/leistungen/mobile-solutions/
- MobileIron
  http://smartling.mobileiron.com/en/germany
- Sophos (smartMan)
  Link siehe in der Linksammlung unter
  https://bvdnet.de/bvd-news-links.html
- Sybase (Afaria)
  http://www.sybase.de/mobilize
- Symantec (Endpoint Protection, Mobile Management, Access Control, SafeGuard Easy)
  http://www.symantec.com/de/de/theme.jsp?themeid=sep-family
  http://www.symantec.com/de/de/mobile-management
  http://www.symantec.com/de/de/network-access-protection
  http://www.symantec.com/business/support/index?page=content&id=TECH30951
- T-Systems (SiMKO)
  http://www.t-systems.de/tsip/de/754852/start/branchen/oeffentlicher-sektor/aeussere-innere-sicherheit/aeussere-innere-sicherheit
- Thinking Objects (Auralis)
  http://www.to.com/auralis.988.0.html
- Ubitexx (ubi-Suite)
  http://www.ubitexx.com/language/de-de/products/multiplatform_management

BYOD kann eingesetzt werden, allerdings müssen

Fazit

viele Bereiche geregelt werden:

- Wie kann zwischen geschäftlichen und privaten Daten unterschieden werden?
- Wie sieht das Archivierungskonzept aus?
- Wie erfolgt eine Synchronisation zwischen mobilem Endgerät und Daten im Unternehmen?
- Wie werden Einsicht-, Nutzungs- und Zugriffsrechte des Arbeitgebers auf die privaten mobilen Endgeräte geregelt?
- Welche Software darf auf dem mobilen Endgerät installiert werden?
- Welche Sicherheitsrichtlinien gelten für private mobile Endgeräte?
- Welche Sicherheitssoftware muss auf den mobilen Endgeräten installiert sein?
- Wer trägt die Lizenzkosten?
- Welche Art der Verschlüsselung wird eingesetzt?

Diese Fragen können nur mit einer Betriebsvereinbarung geregelt werden, zudem ist der Einsatz einer Mobile-Device-Management-Lösung erforderlich. Werden die Sicherheitsrichtlinien entsprechend den Anforderungen des Arbeitgebers bzw. des Unternehmens umgesetzt, werden die Möglichkeiten des Besitzers des mobilen Endgerätes drastisch eingeschränkt:

- er kann nicht jede beliebige App installieren,
- ein Jailbreak oder ähnliches ist ihm nicht erlaubt, damit ist der Zugriff auf verschiedene Möglichkeiten (andere Apps, erweiterte Funktionalität des mobilen Endgerätes durch Nutzung alternativer Firmware) nicht möglich.

Ob der Besitzer des Gerätes dann noch die ursprünglich mit dem Kauf erhoffte Freude am Besitz des Gerätes hat? Oder ob er und auch das Unternehmen sich dann auch die Frage stellt, wofür die Abkürzung BYOD eigentlich steht?

Literatur

Koch FA. (2008) Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel. NZA: 911ff
Koch FA. (2012) Arbeitsrechtliche Auswirkungen von „Bring your own Device" - Die dienstliche Nutzung privater Mobilgeräte und das Arbeitsrecht. ITRB: 35ff
Kremer S, Sander S. (2012) Bring your own Device - Zusammenfassung und Fortführung der Beiträge in ITRB 11/2011 bis ITRB 11/2012. ITRB: 275ff
Söbbing T, Müller NR. (2012) Bring your own Device: Haftung des Unternehmens für urheberrechtsverletzenden Inhalt - Absicherung einer urheberrechtskonformen Hard- und Softwarenutzung für Unternehmenszwecke. ITRB: 15ff
Söbbing T, Müller NR. (2012) Bring your own Device: Strafrechtliche Rahmenbedingungen - Vorkehrungen gegen Datenmissbrauch bei Nutzung privater Geräte im Unternehmen. ITRB: 263ff

Autor

Bernd Schütze
- im Datenschutz für das Gesundheitswesen seit 1995 aktiv,
- Ausbildung: Diplom Informatik, Staatsexamen Medizin, Bachelor of Law, promoviert im Gebiet der Teleradiologie,
- Absolvent der udis,
- Autor diverser Veröffentlichungen zum Bereich Datenschutz und IT-Sicherheit im medizinsichen Umfeld,
- Leiter der AG „Datenschutz in Gesundheitsinformationssystemen" der GMDS

3. privacyGUARD-Kundentag

Praxislösungen für ein konstruktives Datenschutz-Management

Autorin

Nicole Rempe
IT-Bachelor
otris software AG
Königswall 21, 44137 Dortmund
Tel: 0231 . 95 80 69 -70
Fax: 0231 . 95 80 69 -44
E-Mail: rempe@otris.de

Beim dritten privacyGUARD-Kundentag der otris software AG standen praxiszentrierte Lösungen für den betrieblichen Datenschutz im Mittelpunkt. Die knapp 40 Besucher erhielten in einem ausgewogenen Vortragsprogramm spannende Einblicke, Erfahrungsberichte und Anregungen aus erster Hand.

Wilfried Reiners von PRW eröffnete die Veranstaltung mit einem polarisierenden Vortrag. Daten sollen als Werte erkannt und nur in Abwägung der Gegenleistung preisgegeben werden. Der Datenschutzbeauftragte müsse zukünftig eine beratende und überwachende Rolle einnehmen. Im Anschluss stellte die Firma TWINSOFT biometrische Verfahren wie Handvenenerkennung oder Fingerabdruckverfahren vor. Unternehmensberater Thomas Floß demonstrierte auf erfrischende Art, dass Mitarbeitersensibilisierung zu Datenschutz, IT-Sicherheit und Medienkompetenz keine trockene Angelegenheit sein muss: Griffige Beispiele und satirische Videos helfen, ein gesundes Bewusstsein für die Wichtigkeit der Themen zu schaffen. Anschließend beleuchtete Claus Wissing von WIR Solutions kritisch die Datensicherheit in deutschen Unternehmen und gab Empfehlungen zur Risikominimierung. Ingo Ritter vom Konzerndatenschutz der Deutschen Bahn gab einen interessanten Einblick in das Datenschutz-Management des Konzerns, das von 120 Koordinatoren bundesweit geleistet wird. Auf Basis von privacyGUARD laufen Verfahrensmeldungen sowie die Qualifizierung der Verfahren im DB-Konzern vollständig elektronisch ab. Im Schlussvortrag stellten Dr. Christoph Niemann, Vorstand der otris software AG, und Produktmanagerin Nicole Rempe weitere Projektlösungen vor, die otris im privacyGUARD-Umfeld realisiert hat. Natürlich erfuhren die Besucher auch alles über die nächsten privacyGUARD-Versionen.

Unternehmensberater Thomas Floß stellte seine Ideen für eine effektive Mitarbeitersensibilisierung zum Datenschutz vor.

Die Zeiten zwischen den Vorträgen nutzten die Teilnehmer zum regen Austausch von eigenen Erfahrungen und Ideen. Individuelle Fragen und Projektanforderungen erörterten die Besucher direkt im Dialog mit den privacyGUARD-Experten. Auch im kommenden Jahr wird die otris ihren Kunden wieder einen Datenschutztag anbieten, und zwar am 17. September 2014.

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.
- Mehrmandantenfähig
- Modularer Aufbau (Konzern-Modul, Web-Oberfläche, Mehrsprachigkeit etc.)

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

Eine gute Adresse für Datenschutz: www.zd-beck.de

ZD – die Zeitschrift für Datenschutz

informiert umfassend über datenschutzrechtliche Aspekte aus allen Rechtsgebieten. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B. ■ Konzerndatenschutz ■ Beschäftigtendatenschutz ■ Datenschutzaudit ■ Compliance ■ Kundendatenschutz ■ Einwilligung ■ Adresshandel ■ Telekommunikation ■ Soziale Netzwerke ■ Datentransfer in Drittstaaten ■ Vorratsdatenspeicherung

Die ZD-Homepage: www.zd-beck.de

- Editorial/Kontrovers: führende Köpfe kommentieren aktuelle Themen
- Rezensionen/Tagungsberichte
- Nachrichtenarchiv
- Materialien zum Datenschutz

ZD – mehr als eine Zeitschrift

Abonnenten der ZD profitieren von ebenso umfassender wie zeitgemäßer Information:

- monatliche Zeitschrift
- zweimal im Monat Newsletter ZD-Aktuell per E-Mail
- Datenbank ZDDirekt – das komplette Online-Archiv ab der ersten Ausgabe
- ZD-Community

… alles inklusive!

Leseprobe: www.zd-beck.de

Fax-Coupon

☐ **Ja, ich will die ZD inklusive online-Angebot und Newsdienst ZD-Aktuell testen.**
Schicken Sie mir die nächsten 3 Hefte der ZD gratis zu.
Wenn ich nicht bis 1 Woche nach Erhalt des 3. Heftes abbestelle, will ich die ZD im Abonnement.

ZD – Zeitschrift für Datenschutz
3. Jahrgang 2013. Erscheint monatlich mit Newsletter ZD-Aktuell als E-Mail zweimal im Monat.

Jahresabonnement € 199,–.
Vorzugspreis für Abonnenten der Zeitschrift MMR und des beck-online Moduls Multimediarecht € 149,–.
Vorzugspreis für Mitglieder von Kooperationspartnern sowie für Studenten und Referendare € 99,–.
Abbestellung bis 6 Wochen vor Jahresende.
Preise jeweils inkl. MwSt. zzgl. Vertriebs-/Direktbeorderungsgebühren Inland (€ 11,50/€ 2,80) € 14,30 jährlich.

Name

E-Mail (unbedingt erforderlich für den E-Mail-Dienst)

Straße

PLZ/Ort

Datum/Unterschrift 158812 / www

250 Jahre
C.H.BECK

Bestellen Sie bei Ihrem Buchhändler oder bei:
beck-shop.de oder Verlag C.H.BECK · 80791 München
Fax: 089/38189-358 · www.beck.de

Die neue Dimension der Datensicherheit

Online-Kommunikation nicht über jeden beliebigen Cloud-Dienst

In deutschen Datenzentren sind die Daten am besten geschützt. So denken viele Anwender nach den Medienberichten der letzten Monate. Sie wechseln zu einheimischen Cloud-Diensten und sind davon überzeugt, datenschutztechnisch alles getan zu haben. Doch Datenzentrum ist nicht gleich Datenzentrum, auch in Deutschland nicht. Ein genauer Blick tut not.

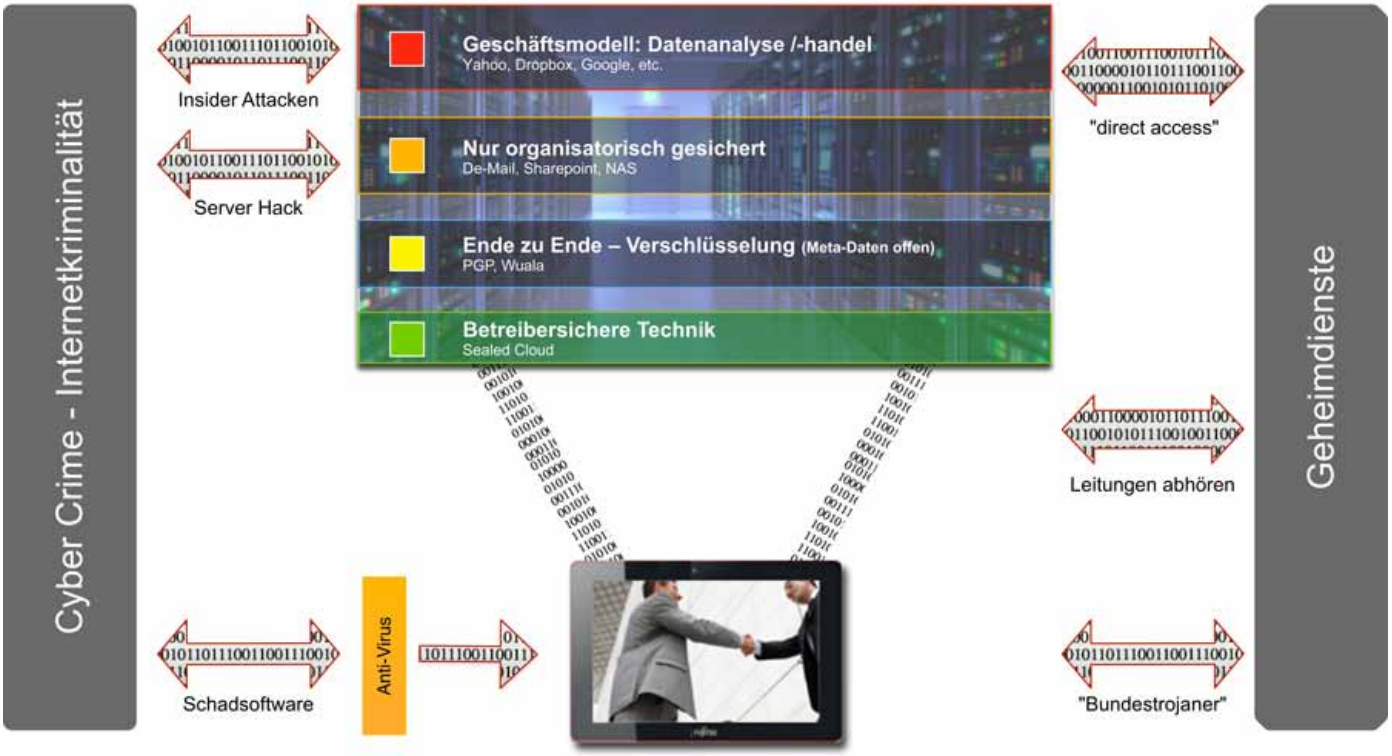
„Unternehmen wissen, dass sie die Online-Geschäftskommunikation nicht von jedem beliebigen Cloud-Dienst erledigen lassen können", sagt Dr. Ralf Rieken, IT-Sicherheitsexperte und Geschäftsführer des Münchner Unternehmens Uniscon GmbH. Trotzdem fallen manche auf die Werbung über die „hohen Sicherheitsstandards" von Anbietern herein und vermeiden einen tieferen Blick in die Technologien, die hinter den Versprechungen stecken. „Das sollten sie aber", meint Rieken, „denn im Bereich der Datensicherheit hat sich ein Quantensprung vollzogen".

Als Entscheider in Sachen Datenschutz müsse man laut Rieken ein komplexes System im Auge behalten, das sich aus dem Transport der Daten, der Speicherung in der Datenbank und der Verarbeitung zusammensetzt. Diese Abläufe werden generell durch technische und organisatorische Maßnahmen abgesichert, die zusammen letztendlich den Grad der Sicherheit eines Online-Dienstes bestimmen. Denn, so Rieken, „eine Sicherheitskette ist nur so stark wie ihr schwächstes Glied." Dabei gilt die Datenverarbeitung zurzeit noch als eine schwache Stelle, weil die Daten bei allen Rechenzentren auf den Anwendungsservern unverschlüsselt vorliegen. Das Risiko, dass diese von Mitarbeitern des Dienstbetreibers selbst missbräuchlich kopiert werden, ist – wie viele Datenskandale belegen – hoch. Daher sichern sich Betreiber, die Sicherheitsrisiken minimieren wollen, gerade in diesem Bereich mit organisatorischen Maßnahmen ab. Die von Uniscon entwickelte und weltweit zum Patent angemeldete Basistechnologie Sealed Cloud „hindert nun technisch den Betreiber daran", erklärt Rieken, „Zugriff auf die Daten zu haben". Die Sealed Cloud, die von Uniscon gemeinsam mit der Fraunhofer Einrichtung AISEC und dem Unternehmen SecureNet im Rahmen des Trusted Cloud Programms des Bundeswirtschaftsministeriums (BMWI) weiter entwickelt wird, ist eine Basistechnologie, welche die Daten des Anwenders auch während der Verarbeitung auf dem Server schützt.

Technischer Schutz auch bei Verarbeitung

Damit die Daten von Applikationen in einem Datenzentrum bearbeitet werden können, sind sie auf dem Anwendungsserver unverschlüsselt. Wenn – wie bei jeder Infrastruktur – ein Wartungsingenieur auf die Server zugreifen muss, so wird bei der Sealed Cloud dafür gesorgt, dass diese Daten zuvor auf einen anderen Server transportiert und auf dem alten Server gelöscht werden. Gleiches gilt bei eventuellen Angriffen auf die Server.

Alle Daten sind in der Datenbank bzw. im Storage-System verschlüsselt gespeichert. Bei den gängigen technischen Lösungen auf hohem Niveau verschlüsselt man die Daten im Storage-System auf Block-Ebene d. h. im Storagetreiber des Betriebssystems mit einem oder wenigen gültigen Schlüssel(n). Die Betreiber bewahren diese dann in (hoffentlich sicheren) Schlüsselspeichern im System auf. Bei der Sealed Cloud Technik geht man da weiter: Das System generiert für jede Anwendersession einen individuellen Schlüssel aus den Login-Informationen. Wenn ein Anwender sich am Ende der Session abmeldet, werden die Daten neu verschlüsselt und gespeichert. Den individuellen Schlüssel zerstört das System. In der Datenbank ist daher für jeden Nutzer der Datensatz jeweils individuell nach AES256 verschlüsselt. Da die Schlüssel im System nicht existieren,



So sicher sind Datenzentren.

ist das Schutzniveau hoch. Angreifer müssten den AES256 entschlüsseln und dies separat für jeden einzelnen Nutzerdatensatz.

Das Zertifizieren von Prozessen und Abläufen

Mehrere Kontrollinstanzen arbeiten bereits an der Attestierung der beschriebenen „Versiegelung" der Sealed Cloud. Laut Rieken forschen die Entwickler zusammen mit einer neutralen Zertifizierungsstelle zusätzlich an einer „Dynamischen Attestierung". Mit ihr soll auch bei laufendem Betrieb geprüft werden, ob sich das System normal verhält und so alle Voraussetzungen für den zertifizierten Ablauf erfüllt sind. Abweichungen würden dazu führen, dass die betroffenen Server sofort außer Betrieb genommen werden. Das System würde den Fehler dann an die zertifizierende Stelle melden.

Auftragsdatenvereinbarung

Angesprochen auf §11 Abs. 2 BDSG, die Auftragsdatenvereinbarung, betont Rieken: „Datenschutz ist eine Kernkompetenz von Uniscon, daher verbinden wir die Pflichten aus §11 und modernes Cloud-Computing." So steht eine Mustervereinbarung online zur Verfügung, gleich neben den Allgemeinen Geschäftsbedingungen des auf Basis der Sealed Cloud entwickelten Kommunikationsdienstes IDGARD (www.idgard.de). Mit ihr könnten Unternehmen mit Uniscon vereinbaren, welche Maßnahmen zum Schutz der Daten vorgenommen werden. „Denn generell gäbe es bei der Online-Kommunikation zwischen Unternehmen", so Rieken, „viele Risikofaktoren für die Sicherheit und damit die Daten".

Er zählt einige auf: „Erstens, dass von vielen verschiedenen Endgeräten (Smartphone, Tablet etc.) aus gearbeitet wird; dass heute sensible Dokumente mehrheitlich per E-Mail unverschlüsselt verschickt werden; dass für firmenübergreifende Teams externe File Sharing Dienste benutzt werden, die den Sicherheitsanforderungen von Unternehmen nicht genügen". Über IDGARD könne man Dokumente und Nachrichten ohne diese Sicherheitsrisiken austauschen, weil der Dienst auf der Sealed Cloud basiert. Rieken: „Unternehmen können damit ohne Softwareinstallation sicher über das Internet kommunizieren – ein Browser genügt. Für Smartphones und Tablets gibt es passende Apps."

Information

Claudia Seidl
Uniscon GmbH
Agnes-Pockels-Bogen 1,
80992 München
E-Mail: claudia.seidl@uniscon.de
Tel: 089 . 41615988-100

So entsteht die „BvD-News“: Von der Idee zum fertigen Heft

Vorschläge externer Autoren sind jederzeit sehr willkommen

Zweimal im Jahr informiert der BvD als Herausgeber mit dem Fachmagazin „BvD-News“ seine Mitglieder, aber auch Aufsichtsbehörden und relevante Ansprechpartner in Behörden, Institutionen und Einrichtungen. Im Magazin finden sowohl BvD-eigene Beiträge Platz als auch externe Beiträge ausgewiesener Experten für den Datenschutz. Produziert wird das Fachmamagzin für den Datenschutz vom Medienhaus Waltrop.

„Der Weg von den ersten Ideen zu Form und Inhalt bis zur finalen Drucklegung und Auslieferung kann mitunter mit einigen Umwegen und Unwägbarkeiten verbunden sein“, erklärt Jürgen Hartz, im BvD-Vorstand mitverantwortlich für die BvD-News. Die eigentliche Planung mit Umfang, Themen und Seitenzahl entsteht in der Regel in einer vorhergehenden Themenkonferenz zwischen BvD-Vorstand und der Redaktion im Medienhaus Waltrop.

„Im Laufe der Produktion ergeben sich aber vielfach weitere interessante Ansätze und Anfragen“, erklärt Jürgen Hartz. Viele Themen sind so relevant, dass die Heftplanung grundlegend verändert wird – nicht selten auch mehrfach während der gesamten Produktion. In dieser

Aus aktuellen Gründen kann sich die Heftstruktur immer wieder ändern. Hier arbeitet Redakteurin Romina Suliani am Interview von Rudi Kramer mit Jan Philipp Albrecht.

Ausgabe ergab sich beispielsweise kurzfristig die Möglichkeit, ein Interview mit MdEP Jan Philipp Albrecht zu platzieren. „Die Möglichkeit haben wir ergriffen und das Interview vorne im Heft eingeplant“, erklärt Redakteur Michael Braun.
Nachdem das Interview von BvD-Vorstand Rudi Kramer geführt wurde, musste es entsprechend erfasst und freigegeben werden. Danach erfolgte die Umsetzung im Layout. Im Layout werden auch die Anzeigen und die redaktionellen Stücke zusammengeführt. Auch dadurch können sich nochmals Veränderungen ergeben: Anzeigengrößen ändern sich, Textbeiträge sind kürzer oder länger als gedacht, so dass hier und da noch einmal umgeplant werden muss.

Online die aktuelle Ausgabe bequem durchblättern

Am Ende einer jeden Heftproduktion steht das Lektorat und das Korrektorat durch Frank Spaeing. Nach einem zweiten Korrekturlauf steht dann das finale Dokument, das in den Druck gegeben werden kann. Bis zur endgültigen Auslieferung sind es dann noch einmal etwa zehn bis zwölf Werktage.

In der Zeit findet parallel die Umsetzung des Magazins für die Webseite des BvD statt. „Eine einfache 1:1-Umsetzung der Druckdatei ins Internet ist nicht möglich, da das Dokument für den Druck optimiert ist“, erklärt Michael Braun. Entsprechend hochauflösend sind die Fotos, so dass bei der Dateierstellung große Datenmengen anfallen.

Für das Internet werden deswegen zwei weitere Versionen in kleinerer Auflösung produziert. „Wir bieten einmal eine pdf mit dem kompletten Heftinhalt zum Download auf https://www.bvdnet.de an, dazu gibt es eine besondere Online-Version, die der Leser komfortabel auf dem Bildschirm lesen kann und in der online geblättert werden kann“, sagt Michael Braun.

Planungen für 2014 laufen: Themen, Termine und mehr

Aktuell laufen die Planungen für die Ausgaben im Jahr 2014. „Wir streben an, erstmals drei Ausgaben im Jahr herauszubringen“, erklärt Jürgen Hartz. Spannende Themen gebe es genug, und durch die Platzierung von Fachbeiträgen in den BvD-News ergeben sich vielfach neue Denkanstöße und Umsetzungsideen für die BvD-Mitglieder. Auch ist der Abstand zwischen den Ausgaben dann nicht mehr so groß, so dass man kurzfristiger auf aktuelle Trends und Diskussionen eingehen kann – wichtig zum Beispiel beim laufenden Prozess zur Erarbeitung der EU-DS-GVO.

Hinweis: 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“, sagt BvD-Vorstand Jürgen Hartz. „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“, sagt Michael Braun. Geschickt werden kann der Vorschlag, die Idee oder das Manuskript einfach per E-Mail an die Redaktionsadresse bvd-news@bvdnet.de.

Gut schreiben können Sie auch lesen:

Das Schreibbuch.

Jetzt in 2. Auflage.

Ein guter Text will gut geschrieben sein. Wie das geht, steht im Schreibbuch. Erfahrene Journalisten und Texter schreiben über das, was sie am besten können. Und beantworten damit Fragen, die sich nicht nur dem Schreib-Anfänger stellen:

- *Wie schreibe ich einen interessanten Vorspann?*
- *Wie erfinde ich eine gute Überschrift?*
- *Was sollte ich bei Teasern beachten?*
- *Wie setzte ich Metaphern und Ironie korrekt ein?*
- *Wie löse ich eine Schreibblockade auf?*
- *Wie schreibe ich einen Text mit Herzblut?*
- *Wie finde ich den Stil, den mein Auftraggeber von mir erwartet?*
- *und noch Vieles mehr, jetzt in:*

Das Schreibbuch.

ISBN 978-3-936083-08-8.

Das sagen Fachleute über das Buch:

„Das Schreibbuch widmet sich dem Thema Schreiben so umfassend, dass kaum eine Frage offenbleibt.“ (WEKA Verlag, HLK)

„Sehr nützlich, sehr empfehlenswert. Unbedingt kaufen und lesen!“ (handling 3/2009)

„Nutzertiges, kurzweiliges Buch, das Profis für die Praxis geschrieben haben.“ (Wissen & Wirtschaft 12/2008)

Alle Infos und Auszüge auf:

das-schreibbuch.de

MEDIEN HAUS WALTROP

„Datenschutz live“: Neue BvD-Reihe startet mit Rhenus

Verband ermöglicht BvD-Mitgliedern mit neuer Veranstaltung einen Blick hinter die Kulissen von Unternehmen

Der BvD hat ein neues Projekt gestartet, um Mitgliedern die Möglichkeit zu geben, hinter die Kulissen von Unternehmen zu schauen. „Datenschutz live“ heißt die neue Veranstaltungsreihe, bei der Unternehmen aus dem Datenschutz im Mittelpunkt stehen. Dabei soll es sich um Firmen handeln, die Produkte oder Dienstleistungen zum Datenschutz anbieten. Die Gelegenheit zur Umsetzung der Idee ergab sich im Sommer als Erstes mit der Rhenus Office Systems, die dem BvD anbot, an sechs Standorten die verschiedenen Bereiche der Entsorgung, Aktenarchivierung und Dokumentenverfilmung im Detail in Augenschein zu nehmen.

Die BvD-Vorstände – hier Jürgen Hartz und Thomas Spaeing – standen den Besuchern bei Rhenus gerne Rede und Antwort.

Der erste Termin startete am 20. Juni in der Leverkusener BayArena. An allen Standorten wurden vor der Unternehmensbesichtigung Fachvorträge zu Datenschutzthemen angeboten. „Für die meisten Termine haben wir dafür auch Vertreter der Aufsichtsbehörden gewinnen können“, erklärt der stellvertretende BvD-Vorstandsvorsitzende Jürgen Hartz, der die Reihe mit konzipiert hatte. Die Themen der Referenten boten von Informationen zur neuen DIN 66399 und zur Datenträgerentsorgung über Herausforderungen und Umsetzung bei der Auftragsverarbeitung bis zur Prüfpraxis der Datenschutzaufsicht ein breites Feld an sachkundigen Informationen. Zu Beginn jeder Veranstaltung berichteten BvD-Vorstände über die aktuelle Situation und Entwicklung der EU-DSGVO und warben für die Stärkung des Be-

Datenschutz zum Anfassen: Rhenus gewährt in der Reihe „Datenschutz live“ einen interessanten Blick hinter die Kulissen. (Foto: Jürgen Hartz)

Gerhard Friederici, Datenschutzbeauftragter für die Rhenus Office Systems, sprach zum Auftakt in Leverkusen über die sichere Archivierung von Informationen. (Fotos: Michael Braun)

rufsbildes und des Berufs des Datenschutzbeauftragten. Wer sich der Registrierung und Zutrittskontrolle mit Identitätsprüfung unterzog und die Vertraulichkeitserklärung unterschrieben hatte, konnte nach den Vorträgen bei den Führungen durch die verschiedenen Unternehmensbereiche besichtigen.

Die Folien aller Vorträge stehen am Ende der Veranstaltungsreihe auf einer gesonderten Seite der BvD-Webseite zur Verfügung. Die Web-Adresse wird den Teilnehmern im Nachgang der Veranstaltungen mitgeteilt. Interessierte Mitglieder können diese auch bei der Geschäftsstelle erfragen.

„Durchschnittlich nutzten jedes Mal über 80 Teilnehmer aus Interessenten und BvD-Mitgliedern das Angebot. Neben dem fachlichen Teil wurden in den Pausen, in denen Rhenus die Teilnehmer sehr gut verköstigte, neue Kontakte geknüpft und Fachgespräche geführt“, sagt Jürgen Hartz. Dabei entstand auch die Idee für einen Runden Tisch zur Datenträgerarchivierung (siehe gesonderter Bericht in dieser Ausgabe). An allen Veranstaltungen konnten Vorstände des BvD zudem Gespräche über die Aktivitäten des Verbandes und die DSgzS-Aktion führen und so neue Mitglieder gewinnen.

Die letzten Veranstaltungen finden am 15. Oktober in München und am 23. Oktober in Stuttgart statt. Infoflyer und Anmeldungen finden sich auf https://www.bvdnet.de/fortbildungen.html

Hinweis: Die erfolgreich gestartete Reihe soll im nächsten Jahr fortgesetzt werden. Dafür sucht der BvD noch interessierte Unternehmen. Diese wenden sich bitte telefonisch oder per Mail an die BvD-Geschäftsstelle.

Ex-BvD-Vorstand Marco Biewald nannte wertvolle Beispiele aus seiner Praxis.

Sichern Sie sich Ihren Schutzengel

Die ByteAction Gruppe ist seit übe
20 Jahren richtungsweisender Hersteller von

- E-Mail-Archivierungssoftware
  - für Rechenzentren — **mandantenfähig**
  - für kleine und mittelständische Unternehmen.

Leistungsspektrum umfasst:

- Spamfilter, Virenschutz & Content-Filter
- Planung, Konzeptionierung sowie Implementierung von Netzwerken & Sicherheitspaketen (Routerkonfiguration)
- Programmierung und Anbindung von Datenbanken und Internetlösungen

Unsere Produkte:

- **BytStorMail** - E-Mail-Archivierung
- **MAV²** - Mail- & Workflow-Management
- **ByteActionMail** - E-Mail-Verschlüsselung (E-Mail, wie ein Einschreiben)
- **SALVUS** - SMS-Warnplattform (Workplace violence / Amokalarm)
- **TaskWatcher** - Workflow-Management Arbeitsabläufe transparent gestalten

ByteAction – Ihr Spezialist für E-Mail-Systeme & Sicherheitssoftware

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft

Fragen Sie uns!
ByteAction GmbH
Auf der Beune 83 – 85
64839 Münster bei Dieburg
Tel.: (0 60 71) 92 16 0
Fax: (0 60 71) 92 16 20
E-Mail: sales@byteaction.de
www.byteaction.de

ByteAction GROUP of Internet Companies

Experten drängen auf ein hohes Datenschutzniveau

Rückblick auf die erfolgreichen BvD-Datenschutztage 2013

Wie geht es weiter mit der geplanten EU-Datenschutzgrundverordnung (EU-DSGVO)? Welche Einwirkungen sind aus deutscher Sicht möglich? Wann kann sie verabschiedet werden? Drängende Fragen zur für den Datenschutz in der Zukunft so wichtigen geplanten EU-Verordnung diskutierten auf den BvD-Datenschutztagen sachkundige Experten und hochrangige Politiker.

Die Bundesministerin der Justiz, Sabine Leutheusser-Schnarrenberger (FDP), plädierte für die Verabschiedung einer europäischen Datenschutz-Regelung noch vor der EU-Wahl 2014. Jan Philipp Albrecht (Bündnis 90 / Die Grünen), Mitglied des Europäischen Parlamentes und dessen Verhandlungsführer für die Verordnung, hofft auf eine Einigung zur Reform im Ministerrat bis April 2014. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, wies auf die Wichtigkeit der Datenschutzbeauftragten für Unternehmen hin, die auch in der EU-DSGVO entsprechend verankert werden müsse. Michael Frieser, Hauptberichterstatter für den Beschäftigtendatenschutz der CDU/CSU-Bundestagsfraktion, forderte Regelungen ein, die effizient für Datenschutzbeauftragte umzusetzen seien. Chris Newiger, Konzerndatenschutzbeauftragte der Deutschen Bahn AG, stellte fest, dass in ihrem Konzern unabhängig von zukünftigen Regelungen grundsätzlich ein hohes Niveau in Sachen Datenschutz etabliert bleibe. Über 200 interne und externe Datenschutzbeauftragte, Vertreter der Aufsichtsbehörden sowie Gäste folgten der Einladung zu den BvD-Datenschutztagen in das NH Hotel Berlin Mitte. Über eine Live-Schaltung nach Brüssel interviewte BvD-Vorstand Rudi Kramer den EU-Abgeordneten Jan Philipp Albrecht, der einen Einblick in die aktuellen Entwicklungen rund um den EU-Kommissionsbeitrag zu einer Reform des europäischen Datenschutzrechts gab. „Bislang sind 3.133 Änderungswünsche zu dem Kommissionsbeitrag eingegangen“, berichtete Albrecht. Eine endgültige Fassung konnte deshalb nicht – wie ursprünglich vorgesehen – Ende Mai an den Ministerrat und das EU-Parlament überreicht werden. Stattdessen hofft der Berichterstatter des Ausschusses LIBE (Bürgerliche Freiheiten, Justiz und Inneres) auf eine Einigung zur Reform bis April 2014. „Danach halte ich eine Anpassungszeit von zwei Jahren für angemessen, das bedeutet, ab Mitte 2016 sollten die Regeln angewendet werden.“

Auch Bundesjustizministerin Sabine Leutheus-

Bundesjustizministerin Sabine Leutheusser-Schnarrenberger plädierte für die Verabschiedung einer europäischen Datenschutz-Regelung vor der EU-Wahl 2014. Der stellvertretende BvD-Vorstandsvorsitzende Jürgen Hartz moderierte die Veranstaltung gemeinsam mit BvD-Vorstand Rudi Kramer, rechts im Gespräch mit Michael Frieser.

ser-Schnarrenberger plädierte für die Verabschiedung einer europäischen Datenschutz-Regelung noch vor der EU-Wahl 2014. Ihrer Meinung nach schafft eine europaweit einheitliche Regelung Rechtssicherheit für Unternehmen: „Deswegen ist die EU-DSGVO ein wichtiges Projekt - auch unter wirtschaftlichen Gesichtspunkten“, sagte Leutheusser-Schnarrenberger. Den Bereich des Beschäftigtendatenschutzes schätzt die FDP-Politikerin als „immer wichtiger“ ein. Somit stiegen die Anforderungen an die betrieblichen Datenschutzbeauftragten. Auch deshalb sei eine einheitliche Regelung sinnvoll. Mit einer Öffnungsklausel in der Grundverordnung bliebe die Möglichkeit bestehen, die Regelung individuell anzupassen.

Einen ähnlichen Standpunkt nahm Michael Frieser, Hauptberichterstatter für den Beschäftigtendatenschutz der CDU/CSU-Bundestagsfraktion, ein. Entscheidende Rahmenbedingungen für den Beschäftigtendatenschutz könne die EU-DSGVO vorgeben. Seine Kritik am aktuellen Entwurf: „Was uns umtreibt, ist der Unterschied im Abstraktionsniveau.“ Man müsse Regelungen finden, die effizient für Datenschutzbeauftragte umzusetzen sind.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, hielt ein Plädoyer für eine differenzierte Sichtweise auf den Gesetzesentwurf der EU-Kommission und stellte die Wichtigkeit der Datenschutzbeauftragten für Unternehmen heraus. „Datenschutzbeauftragte sind Teil des Managementprozesses, und deswegen müssen sie gestärkt werden“, sagte Schaar. Die Datenschutzbeauftragten bildeten eine wichtige Schnittstelle zwischen den Unternehmen, der Allgemeinheit und den Aufsichtsbehörden. Für eine Datenschutzverordnung sei es deshalb wichtig, einen hohen Mindeststandard festzulegen. „Schlimmer als ein Scheitern des Entwurfes wäre eine Vollharmonisierung auf niedrigerem Niveau, in der die Grundrechtsituation abgesenkt wird“, stellte Schaar klar.

Am Nachmittag vertieften die Besucher der BvD-Datenschutztage die aufgeworfenen Themen in 15 verschiedenen Workshops. Am Vortag hatten viele BvD-Mitglieder schon das Angebot angenommen, verschiedene Sonderseminare zu belegen. Auch hier lagen die Anmeldezahlen auf einem sehr hohen Niveau. „Die starke Resonanz auf die BvD-Datenschutztage und die deutlichen Statements der prominenten Redner haben gezeigt, wie wichtig die anstehende Entscheidung zur EU-DSGVO für viele gesellschaftliche Bereiche ist und wie sinnvoll es ist, entsprechend intensiv an der Ausgestaltung der Verordnung mitzuarbeiten“, erklärte der stellvertretende Vorstandsvorsitzende des BvD, Jürgen Hartz, im Nachgang zur Veranstaltung. Deswegen gelte es jetzt, mit politischen und wirtschaftlichen Kräften gemeinsam an einer Fassung der Verord-

Sichern Sie sich Ihren Schutzengel

Gesetzeskonforme E-Mail-Archivierung

- ist notwendig, wie „TÜV am Auto“
- hilft für die Beweisfähigkeit bei Rechtsstreitigkeiten
- unterstützt die Einhaltung der Datenschutzrichtlinien
- ist für jedes E-Mail-System geeignet
- kann E-Mails leicht wiederherstellen
- sollte Plattformunabhängig und einfach zu integrieren sein
  - ∗ leichte und unkomplizierte Installation
  - ∗ keine Änderungen an Hard- und Software
  - ∗ kompatibel zu allen Mailservern

Wenn Rechtskonform, dann sind Ihre Kunden gesetzlich auf der sicheren Seite!

BytStorMail ist der Schutzengel für diese Anforderungen.

Mitglieder des BvD erhalten besonderen Support und Unterstützung.

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft

Fragen Sie uns:
ByteAction GmbH
Auf der Beune 83 – 85
64839 Münster bei Dieburg
Tel.: (0 60 71) 92 16 0
Fax: (0 60 71) 92 16 20
E-Mail: sales@byteaction.de
www.byteaction.de

ByteAction GROUP of Internet Companies

Peter Schaar hielt ein Plädoyer für eine differenzierte Sichtweise auf den Gesetzesentwurf der EU-Kommission. Reinhard Alff ließ sich von Statements zu Karikaturen hinreißen. Prof. Gerhard Kongehl (udis) gehörte zu den Besuchern. Auf der parallel stattfindenden Ausstellung führten die Besucher gute Gespräche.

nung mitzuarbeiten, die das hohe Niveau des Datenschutzes in Deutschland bestätige und den Status von Datenschutzbeauftragten entsprechend festige. „Auch der BvD wird mit Informationsveranstaltungen und Stellungnahmen auf die relevanten Punkte des Entwurfs hinweisen sowie den Dialog nach Brüssel weiter intensivieren“, sagte BvD-Vorstandsvorsitzender Thomas Spaeing. Das Symposium am 17. Oktober ist dabei ein wichtiger nächster Schritt.

Das attraktive Programm zu den BvD-Datenschutztagen lockte so viele Teilnehmer an wie noch nie. Die BvD-Mitglieder folgten interessiert den Vorträgen.

Neue Möglichkeiten der Diskussion - der BvD-Blog

AK Social Media stellt das Logbuch für den BvD vor

Das Internet bringt uns tagtäglich eine unüberschaubare Menge an Informationen, die es wert sind, gelesen zu werden. Aber die wenigsten Mitglieder des BvD haben die Möglichkeit, auch nur einen Teil der Neuigkeiten zu erfassen. Eigene Projekte, BvD-Verbandsarbeit und weitere Aktivitäten lassen uns nur begrenzt Zeit. Es wäre toll, wenn es einen Filter geben würde, der uns die wichtigsten Ereignisse aus dem Web 2.0 erfahren lässt - frei nach dem Motto „Wenn es etwas Wichtiges gibt - es wird mich erreichen“. Eine Möglichkeit hier noch Verbesserung zu schaffen, könnte ein zentraler BvD-Blog sein, ein Logbuch der wichtigsten Meldungen – auf der BvD-Webseite publiziert.

Zum BvD-Blog gelangt man über den Link oben rechts auf jeder Seite. Auf der Startseite sind jeweils die letzten fünf Blogbeiträge dargestellt.

Ein Logbuch für den BvD: Dieses Thema wurde als Aufgabe im Arbeitskreis „Social Media“ (AK Social Media) erkannt. Einige der Mitglieder betätigen sich bereits als Blogger in ihren Unternehmen und erkannten den Mehrwert, den es auch für BvD-Mitglieder bringen könnte. Die Idee war geboren, es ging nun um die Freigabe und Etablierung auf der BvD-Webseite, die Administration und die Themen, die sich in dem BvD-Blog wiederfinden sollten.

Die Entstehungsgeschichte: Bereits bei dem ersten Treffen des AK Social Media, in dem es um die grundsätzlichen Aufgaben des Arbeitskreises ging, stand ein möglicher BvD-Blog weit oben auf der Aufgabenliste. Bis zur Version 1.0 war es aber noch ein weiter Weg.

Im Anschluss an die Verbandstage 2013 ging der BvD Blog live. Allerdings war er zu Beginn mehr ein Blog für Insider. Hier konnte getestet werden, wie ein Blog auf der BvD Webseite funktioniert und wo die Besucher der Webseite diesen am besten wahrnehmen. Da die Mitglieder des AK Social Media, genau wie die meisten anderen Besucher der BvD-Webseite, nicht regelmäßig die Webseite auf Änderungen kontrollieren, war eine erste Anforderung an die neue Version über Änderungen am Blog automatisch informiert zu werden. Deshalb wurde ein RSS-Feed eingerichtet.

Außerdem wurde der BvD-Blog so gestaltet,

Sichern Sie sich Ihren Schutzengel

Aus einer E-Mail wird ein Einschreibebrief

Rechtskonform durch Einhaltung der Datenschutzgesetze

Zusätzlich mit E-Mail-Verschlüsselung
Mit ByteActionMail machen Sie aus einer klassischen E-Mail einen vertraulichen elektronischen Brief mit automatischer Empfangsbestätigung, wie dies den Anforderungen im Business-Umfeld entspricht.

Vertrauliche & verbindliche E-Mail-Kommunikation:

- macht normale E-Mail zum sicheren, elektronischen Brief
- Versand und Empfang funktionieren mit jeder E-Mail Adresse und ohne zusätzlichen Aufwand
- automatische Empfangsbestätigung sorgt für Klarheit
- jederzeitige Nachvollziehbarkeit durch Transaktionsregister
- leicht integrierbar in bestehende Unternehmenslösungen

ByteActionMail ist die einfache und sichere Lösung für alle, die die Kommunikation zwischen ihren Mitarbeitern, Kunden, Lieferanten und Geschäftspartnern ernst nehmen wollen.

Fragen Sie uns:
ByteAction GmbH
Auf der Beune 83 – 85
64839 Münster bei Dieburg
Tel.: (0 60 71) 92 16 0
Fax: (0 60 71) 92 16 20
E-Mail: sales@byteaction.de
www.byteaction.de

ByteAction
GROUP of Internet Companies

Den RSS-Feed wird bequem auf der Blog-Seite unter www.bvdnet.de abonniert.

dass jeder Besucher der BvD-Webseite die Blog-Beiträge einfach über soziale Netzwerke wie z. B. über Twitter und XING teilen kann.

Ein abgestimmter Prozess: Zusammen mit dem BvD-Vorstand wurde überlegt, welche rechtlichen Vorgaben und welche Prozesse beachtet werden müssen. Mit den Rechtsexperten im BvD-Vorstand wurden die Rahmenbedingungen abgesteckt, die rechtlichen Vorgaben besprochen und der Prozess definiert, wie neue Blogbeiträge freigegeben und wie Kommentare zu den Beiträgen eingestellt werden können.

Wie entsteht ein Blog-Beitrag?

- Erstellt ein Autor einen neuen Blog-Beitrag, wird dieser per E-Mail an den zuständigen BvD-Vorstand übermittelt
- Der zuständige BvD-Vorstand gibt den Blog-Beitrag frei
- Der Autor stellt den Blog-Beitrag ein
- Leser kommentieren den Blog-Beitrag ;-)
- Kommentare werden dem Autor gemeldet
- Der Autor gibt den Kommentar frei

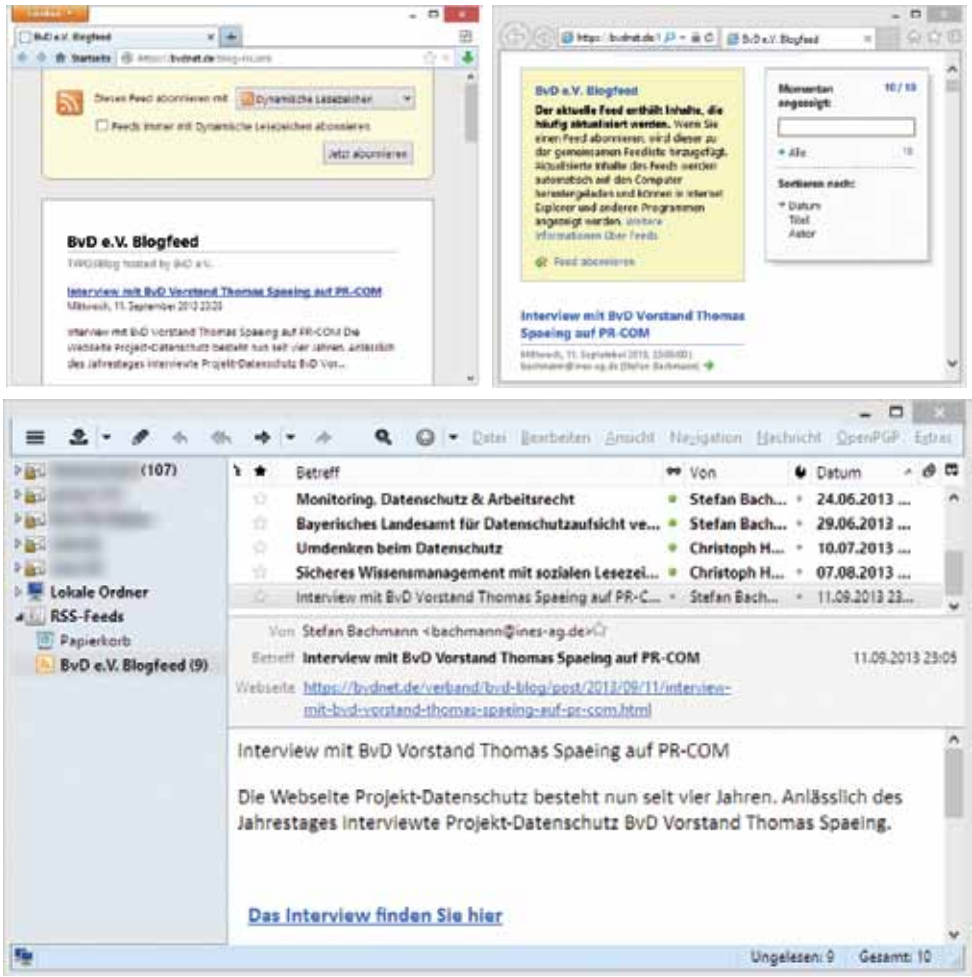
Ihre Mitarbeit entscheidet über die Relevanz: Die verschiedenen Ansichten, Herangehensweisen und praktischen Erfahrungen sind es, die uns Mehrwerte liefern können.
Es liegt an uns allen, den BvD-Blog mit Leben zu erfüllen. Nehmen Sie an der Diskussion teil – beteiligen Sie sich am BvD-Blog!

Wo finde ich den BvD-Blog?
Auf der BvD-Webseite in der rechten, oberen Ecke sehen Sie immer den Link zum BvD-Blog. Auf der Startseite werden in der rechten Spalte die aktuellsten Blogbeiträge gezeigt. Um komfortabel über neue Blogbeiträge informiert zu werden, abonnieren Sie einfach den **RSS-Feed** (siehe Abbildung oben und Infokasten links). Je nach verwendetem Programm sieht der Abonnie-

Information

RSS-Feed

Ein RSS-Feed ist ein Nachrichten-Direktkanal von einer Webseite zu den Besuchern der Webseite. Immer wenn ein neuer Beitrag auf der Webseite veröffentlicht wird, wird er über diesen Kanal losgeschickt - und die Besucher bekommen mit Hilfe praktischer Hilfsprogramme (u.a. Mozilla Firefox, Internet Explorer, Outlook und Mozilla Thunderbird können mit RSS-Feeds umgehen) oder Internet-Seiten eine Meldung. So werden den Besuchern wie bei einem Abo alle Beiträge automatisch zugestellt. Wenn die Besucher im RSS-Feed auf den Link klicken, landen sie automatisch auf der entsprechenden Seite im passenden Beitrag.



Je nach verwendetem Programm kann der Abonnieren-Vorgang unterschiedlich aussehen. Hier im Vergleich Firefox oben links, daneben der Internet Explorer und darunter Thunderbird.

ren-Vorgang anders aus.

Kommentare erstellen: Unter jedem Blog-Beitrag finden Sie die Möglichkeit, durch Klick auf Kommentare Ihre Erläuterung zu diesem Thema einzubringen (siehe Abbildung links).

Automatische Benachrichtigung bei weiteren Kommentaren: Um komfortabel über weitere Kommentare zum Blog-Eintrag informiert zu werden, können Sie am Ende der Seite einen Haken setzen. An die von Ihnen bei der Erstellung des Kommentars eingegebene E-Mail-Adresse werden die Aktualisierungen übermittelt.

Komfortmerkmal für BvD-Mitglieder: Wenn Sie als BvD-Mitglied im Mitgliederbereich angemeldet sind, werden beim Erstellen eines Kommentars die Pflichtfelder (Name und E-Mail-Adresse) schon vorausgefüllt. Natürlich können Sie als BvD-Mitglied auch einen anonymen Beitrag erstellen, indem Sie auf eine vorherige Anmeldung verzichten.

Fazit: Über den BvD-Blog stellt der BvD seinen Mitgliedern (und allen anderen Besuchern der Webseite) eine neue Möglichkeit, wichtige Inhalte zu teilen und zu diskutieren. Lassen Sie uns diese Möglichkeit der Zusammenarbeit nutzen, um uns gegenseitig unser umfassendes Fachwissen verfügbar zu machen. Wenn Sie Fragen und Anregungen zu dem Blog haben, freuen wir uns über eine E-Mail an blog@bvdnet.de oder einen Kommentar im BvD-Blog.

Abonnieren
Ich möchte über jeden weiteren Kommentar in diesem Post benachrichtigt werden.
Ich akzeptiere die Blog-Nutzungsbedingungen.
Kommentar absenden

Autoren

Die Mitglieder des AK Social Media
ak-socialmedia@bvdnet.de.

PETER GOLA

Mitarbeiterbefragungen – datenschutzrechtliche Vorgaben und Grenzen

Offenbarungspflicht und Schweigerecht bei der Datenerhebung

Teilnahme- und Auskunftspflicht
Personenbezogene Erhebung
Fragerecht
„Informierte" Einwilligung
Datenerhebungsrecht

■ Ob bei Mitarbeiterbefragungen eine Teilnahme- und Auskunftspflicht der Beschäftigten besteht, richtet sich nach den zur Erörterung vorgesehenen Themen. Geht es um im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses mitzuteilende Informationen, bestehen Auskunftspflichten, sofern Persönlichkeitsrechte des Beschäftigten nicht entgegenstehen. Werden dagegen allgemeine Auskünfte und Einschätzungen zur Organisation des Betriebs, zum Arbeitsklima oder zur Arbeitszufriedenheit etc. von der gesamten oder Teilen der Belegschaft erbeten, so ist die Teilnahme an der Befragung freiwillig, was regelmäßig deren Anonymität voraussetzt. Eine Einwilligung in eine personenbezogene Erhebung wird in der Regel an der gebotenen Freiwilligkeit scheitern.

■ The question of whether there is an obligation for employees to participate in and provide information for employee surveys is dependent upon the issues to be covered. If the information to be imparted deals with issues regarding the implementation of the employment relationship then there are obligations to disclose information insofar as the employee's personal rights do not stand in opposition thereto. However, if general information and assessments regarding the organization of the company, the working climate or job satisfaction are requested by all or part of the employees, then participation in the survey is voluntary; this also generally stipulates the anonymity thereof. Consent in a survey regarding personal data will generally not succeed due to the obligatory voluntary nature of the same.

I. Vorbemerkungen

Auch im bestehenden Arbeitsverhältnis steht dem Arbeitgeber ein „Fragerecht" gegenüber den Beschäftigten zu.[1] Bestimmt wird der Gegenstand des Datenerhebungsrechts und der korrespondierenden Auskunftspflicht des Mitarbeiters dadurch, dass die Information für die Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG).

Die Erforderlichkeit setzt voraus, dass der Arbeitgeber die Information zur Wahrnehmung seiner Rechte und Pflichten aus dem Beschäftigungsverhältnis benötigt und der Verhältnismäßigkeitsgrundsatz gewahrt ist.

Die Art und Weise, wie die Arbeitnehmer insoweit relevante Informationen dem Arbeitgeber mitzuteilen haben, kann der Arbeitgeber auf Grund seines Direktionsrechts festlegen. Sein Weisungsrecht betrifft zunächst die Konkretisierung der Hauptleistungspflicht. Es ermöglicht dem Arbeitgeber, dem Arbeitnehmer bestimmte Aufgaben zuzuweisen und den Ort und die Zeit ihrer Erledigung verbindlich festzulegen. Seine Befugnis zur Erteilung von Weisungen zur Ordnung und dem Verhalten den Arbeitnehmer im Betrieb (§ 106 GewO) erstreckt sich auch auf die Anordnung zur Teilnahme an Mitarbeitergesprächen.

Voraussetzung ist, dass es sich um eine Angelegenheit handelt, die im Rahmen des Direktionsrechts besprochen werden soll[2] und dass die vom Mitarbeiter erbetenen Informationen sich im Zulässigkeitsrahmen des BDSG bewegen. Stets muss der Arbeitgeber bei Weisungen billiges Ermessen walten lassen. Das schließt die Achtung grundrechtlich geschützter Interessen ein.[3]

Ein Beispiel solcher sich in dem aufgezeigten Rahmen bewegenden Mitarbeitergespräche bilden Mitarbeiterjahres- oder Zielvorgabegespräche.[4] Die vor einer Verdachtskündigung gebotene Anhörung setzt voraus, dass dem Mitarbeiter der Sachverhalt offengelegt wird, zu dem er sich äußern soll.[5] Bestandteil von zur Aufklärung von strafrechtsrelevanten Sachverhalten im Betrieb durchgeführten „Internal Investigations"[6] sind Mitarbeiterbefragungen, wobei es um Aussagen von Zeugen und Verdächtigten geht.

Die Pflicht, zu im Zusammenhang mit seinem Arbeitsverhältnis stehenden Fragen Auskunft zu geben,[7] kann hier im Spannungsfeld mit dem im Strafrecht geltenden Grundsatz stehen, dass niemand sich selbst belasten muss. Ein weiteres Beispiel bil-

1 Zu „Fragerecht und Offenbarungspflicht" im Zusammenhang mit der Begründung des Beschäftigungsverhältnisses vgl. *Gola/Wronka*, Hdb. zum Arbeitnehmerdatenschutz, 6. Aufl., Rdnr. 456 ff.
2 *BAG* NJW 2009, 3115.
3 ErfK/*Preis*, § 106 GewO Nr. 6.
4 Zur fehlenden Erzwingbarkeit von Personalgesprächen vgl. *Bausewein*, RDV 2012, 139.
5 *BAG* DB 2011, 880; *LAG Berlin-Brandenburg*, U. v. 17.2.2011 – 25 Sa 2421/10.
6 Zur Teilnahme und Auskunftspflicht vgl. *Momsen*, ZIS 6/2011, 567, abrufbar unter: ZIS-online.com/dat/artikel/2011_6_586; *Dann/Schmidt*, NJW 2009, 1851.
7 *Göpfert/Merten/Siegrist*, NJW 1998, 1705.

den Krankenrückkehrergespräche. So kann es, wenn ein Mitarbeiter nach wiederholter oder längerer Erkrankung seine Arbeit wieder aufnimmt, angezeigt sein, mit dem Mitarbeiter die weiteren Einsatzmöglichkeiten zu erörtern. Bei der Einladung zu dem Gespräch ist der Betroffene über den Zweck des Gesprächs und die Reichweite seiner Auskunftspflicht zu belehren.

Der Arbeitgeber darf sich nach den Ursachen der Erkrankung und ihrer Heilung „abstrakt" erkundigen, d.h. danach fragen, ob der Mitarbeiter wieder voll einsatzfähig ist oder ob man über eine andere seiner Leistungsfähigkeit entsprechende Verwendung nachdenken solle. Nach konkreten medizinischen Diagnosen darf nicht gefragt werden.[8]

Korrespondierend zu dem Recht des Arbeitgebers, Fragen des Arbeitsverhältnisses oder betriebliche Fragen mit dem Mitarbeiter zu erörtern, steht das Recht des Mitarbeiters, in betrieblichen Angelegenheiten, die seine Person betreffen, von den hierfür zuständigen Personen gehört zu werden. Im Besonderen kann er verlangen, dass die Beurteilung seiner Leistungen sowie die Möglichkeiten seiner beruflichen Entwicklung im Betrieb erörtert werden. Er ist berechtigt, zu Maßnahmen des Arbeitgebers, die ihn betreffen, Stellung zu nehmen sowie Vorschläge für die Gestaltung der Arbeitsplätze und des Arbeitsablaufs zu machen (§ 82 BetrVG).

Im Gegensatz zu diesen „Einzelgesprächen" stehen „pauschale" Mitarbeiterbefragungen der gesamten oder von nach bestimmten Kriterien festlegten Teilen der Belegschaft. Derartige Datenerhebungen sollen helfen, Stärken oder Schwächen eines Unternehmens zu erkennen. Sie dienen zum einen dem Arbeitgeber zur Analyse und Diagnose der erfragten Sachverhalte und zum anderen der Beteiligung der Beschäftigten bei Veränderungs- und Modernisierungsprozessen. Abgefragt werden Bewertungen des Arbeitsumfelds, von Führung und Zusammenarbeit, die Arbeitszufriedenheit oder die Motivation. Gegenstand der Erhebung können auch sensible Tatbestände wie das Gesundheits- und Stressbild der Beschäftigten sein. Gleichwohl ist von Interesse nicht der einzelne Beschäftigte, sondern das Meinungsbild von Teilen oder der Gesamtheit der Belegschaft.

Je nach Zielstellung im Unternehmen ergeben sich verschiedene Formen einer Mitarbeiterbefragung.[9] Dazu zählen:

- Zufriedenheitsumfragen (Erhebung der Zufriedenheit der Mitarbeiter mit verschiedenen Aspekten im Unternehmen)
- Klima-/Kulturbefragung (spezielle Abfrage der Themen Betriebsklima und Unternehmenskultur)
- Engagement-Befragungen (Untersuchung von Performance, Motivation, Bindung und Leistungsfähigkeit der Mitarbeiter)
- Prozess-Evaluationen (Bewertung des Planungsprozesses, Unterstützung des Change Managements)

Die Zulässigkeit derartiger Erhebungen und die Pflicht der Mitarbeiter zur Teilnahme ist Gegenstand der nachfolgenden Betrachtung.

II. Anonyme Datenerhebung

Keine arbeits- und datenschutzrechtlichen Probleme entstehen, wenn die Befragung in anonymisierter Form erfolgt, d.h. der Arbeitgeber nicht erkennen kann, wer an der Befragung teilgenommen bzw. Aussagen zu den Fragestellungen abgelehnt hat. Damit ist dann einerseits auch die Freiwilligkeit der Teilnahme sichergestellt. Zum anderen besteht nicht die Gefahr, dass die Fragen nicht wahrheitsgemäß, sondern „geschönt" beantwortet werden.

Diese Anonymität ist aber nur gewahrt, wenn nicht nachträglich auf Grund der Struktur der Befragung und der jeweiligen Antworten auf bestimmte Beschäftigte rückgeschlossen werden kann. Das ist häufig der Fall, wenn statistische Angaben erfragt werden, etwa zu dem Alter, der Betriebszugehörigkeit, dem Geschlecht sowie nach Voll- oder Teilzeitbeschäftigung und Abteilungszugehörigkeit. Die Informationen können durchaus von Interesse sein, dürfen aber nicht dazu führen, dass eine Rückführung auf die betroffene Person möglich ist.

Derartige Probleme ergeben sich auch, wenn die Befragung online erfolgen soll, da hier der Befragte durch IP-Adresse, Benutzername, Browser Fingerprint und Cookies ermittelt werden kann.[10] Gleiches gilt, wenn die Beantwortung der Fragen aus dem E-Mail-Postfach des Mitarbeiters erfolgt.[11] An dem Personenbezug der Erhebung ändert sich nichts, wenn die Auswertung der erhobenen Daten anschließend aggregiert in Gruppenangaben erfolgt, um damit den Rückschluss auf einzelne Personen auszuschließen.[12]

III. Personenbezogene Datenerhebung

Ist der Personenbezug der Datenerhebung nicht ausgeschlossen, d.h. wenn die Teilnehmer an der Umfrage näher bestimmt oder bestimmbar sind, stellt sich die Frage nach der datenschutzrechtlichen Zulässigkeit.

Vor dem Schritt zur personenbezogenen Datenerhebung steht jedoch zunächst das Gebot der Datenvermeidung und Datensparsamkeit des § 3a BDSG zur Prüfung an, d.h. ob das Umfrageziel nicht auf dem aufgezeigten Weg der anonymen Durchführung der Erhebung erreicht werden kann. Hieraus kann sich auch die Verpflichtung einer Anonymisierung im zweiten Schritt der Erhebung ergeben, d.h. die vom Erhebungsbogen getrennte Erfassung der Daten des Absenders.

Als Rechtsgrundlage für eine personenbezogene Datenerhebung ist § 32 Abs. 1 Satz 1 oder ggf. § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht zu ziehen.

§ 32 Abs. 1 Satz 1 BDSG verlangt, dass die Zweckbestimmung der Datenerhebung im Rahmen der Durchführung des mit dem Beschäftigten bestehenden Arbeitsverhältnisses erforderlich ist. Zur Durchführung des Arbeitsverhältnisses erforderlich sind die Daten, die der Arbeitgeber zur Wahrnehmung seiner Rechte und zur Erfüllung seiner Pflichten gegenüber dem betroffenen Beschäftigten vernünftigerweise benötigt.[13] Für die Durchführung der individuellen Vertragsbeziehung ist die Teilnahme an einer allgemeinen Mitarbeiterbefragung nicht erforderlich.

Der bei Nichtvorliegen der Zweckbestimmung des § 32 Abs. 1 BDSG weiterhin anwendbare § 28 Abs. 1 Satz 1 Nr. 2 BDSG[14] scheidet ebenfalls regelmäßig als Zulässigkeitsnorm aus, da den berechtigten Interessen des Arbeitgebers an der Durchführung der Umfrage zumeist überwiegende schutzwürdige Interessen der Beschäftigten entgegenstehen.

Der Beschäftigte muss dem Arbeitgeber nicht seine subjektive Einschätzung der Arbeitsbedingungen, seine Motivation bzw. stattgefundene „innere Kündigung" oder von ihm empfunde-

8 Vgl. *LfD Baden-Württemberg*, 30. TB 2010/2011, S. 136.
9 Vgl. *SKOPOS GmbH & Co. KG*, Institut für Markt- und Kommunikationsforschung.
10 Zum Ausschluss derartiger Möglichkeiten: *LfD Baden-Württemberg* (o. Fußn. 8), S. 144 f.
11 S. die Hinweise zu diesbezüglichen Anonymisierungsmöglichkeiten: *Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit* (*HambBfDI*), Empfehlungen zum Datenschutz bei Mitarbeiterbefragungen, abrufbar unter: www.datenschutz-hamburg.de.
12 *Bayerisches Landesamt für Datenschutz*, Tätigkeitsbericht (2011/2012), S. 67 f.
13 *Gola/Schomerus*, BDSG, 11. Aufl., § 32 Rdnr. 10 ff.
14 Vgl. *Gola/Wronka* (o. Fußn. 1), Rdnr. 664 ff.

nen Probleme mit der Zusammenarbeit mit Kollegen oder Vorgesetzten offenbaren und damit die Erstellung eines Persönlichkeitsbilds eröffnen. Eine Verpflichtung der Mitarbeiter, dem Arbeitgeber ihre subjektive Meinung über ihre Arbeitsbedingungen mitzuteilen, besteht daher regelmäßig nicht.[15]

Damit bleibt die Frage, ob die Datenerhebung bei den Mitarbeitern zulässig ist, die hierin einwilligen und sich bei eindeutig freigestellter Teilnahme[16] an der Umfrage beteiligen. Eine „informierte" Einwilligung setzt zunächst voraus, dass der Zweck der Befragung, die beabsichtigten Auswertungen und die die Befragung durchführende bzw. die Befragungsergebnisse auswertende Stelle offengelegt werden. Zugesichert werden muss, dass den Beschäftigten im Falle der Nichtbeteiligung keine Nachteile entstehen.[17] Gleichwohl wird die nach § 4a Abs. 1 BDSG erforderliche Freiwilligkeit auf Grund der wirtschaftlichen Abhängigkeit des Arbeitnehmers häufig fraglich sein.[18]

IV. Einschaltung eines Dienstleisters

Die die Freiwilligkeit gefährdende Gefahr eventueller Benachteiligung bei Versagung der Einwilligung kann entfallen, wenn der Arbeitgeber durch Einschaltung eines die Befragung durchführenden und insoweit zur Vertraulichkeit verpflichteten Dienstleisters nicht erfährt, wer an der Befragung teilgenommen hat und ihm die Auswertung der Befragungsergebnisse in hinreichender Aggregierung mitgeteilt[19] und dieses Vorgehen mit einer erforderlichen Betriebsvereinbarung abgesichert wird. Die Einschaltung des Dienstleisters kann sich, je nachdem ob er als „Personalforschungsinstitut" die Befragung in eigener Regie durchführt oder ob er auf Weisung des Arbeitgeber handelt, als Funktionsübertragung oder Auftragsdatenverarbeitung darstellen. Die Frage der Zulässigkeit der Weitergabe von Mitarbeiterdaten an den Dienstleister stellt sich nicht, wenn diese – ggf. in pseudonymisierter Form unter Einschaltung eines Codes – durch den jeweiligen Mitarbeiter erfolgt. Doppelbeteiligungen können hierdurch ausgeschlossen werden.

V. Konzernweite Befragung

Auch wenn der Wunsch der Mitgliederbefragung von der Konzernmutter ausgeht, ist eine Übermittlung der Mitarbeiterdaten an die Konzernmutter, damit von dort die Befragung personenbezogen gestartet werden kann, weder durch § 32 Abs. 1 Satz 1 BDSG noch durch § 28 Abs. 2 Satz 2 BDSG gerechtfertigt. Jedenfalls kann das Streben nach einem einheitlichen Personal-Management oder einer einheitlichen Personalsteuerung allein kein den schutzwürdigen Interessen der Beschäftigten vorrangiges berechtigtes Interesse begründen.

Gemäß dem Aspekt der Freiwilligkeit der Teilnahme genügt es, wenn die Tochter die Mitarbeiter über den Wunsch der Mutter informiert und diese die von der Mutter vorgegeben Fragen unmittelbar beantworten. Dies kann in anonymer oder pseudonymisierter Form erfolgen.[20]

VI. Beteiligung des Betriebsrats

Als Beteiligungsrechte des Betriebsrats kommen vorrangig in Betracht:

1. Informationsrecht des § 80 Abs. 2 BetrVG

Der Betriebsrat kann auch bei nicht mitbestimmungspflichtiger anonymer Befragung Auskunft über die Auswertungsergebnisse verlangen, wenn die hinreichende Wahrscheinlichkeit besteht, dass diese Bezug zu Aufgaben des Betriebsrats haben.[21]

2. Mitbestimmungsrecht bei Personalfragebögen und Beurteilungsgrundsätze nach § 94 BetrVG

Der Einsatz eines „Personalfragebogens" erfolgt, wenn Beschäftigte einer standardmäßigen Befragung unterzogen werden und sich die Fragen auf ihre persönlichen Verhältnisse und nicht auf eine von den Beschäftigten losgelöste Arbeitsplatzbeschreibung erstrecken.[22] Das Mitbestimmungsrecht erfasst den Gegenstand der Fragen ebenso wie den Verwendungszweck der erhobenen Daten. Es gilt unabhängig davon, ob die Beantwortung der Fragen freigestellt ist oder ob die Befragung durch einen Dritten erfolgt.[23] Es entfällt, wenn die Befragung anonym erfolgt.

3. Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG

Erfolgt die Befragung online oder werden die Daten automatisiert ausgewertet, unterliegt das Verfahren so lange der Mitbestimmung, wie ein Personenbezug der Daten vorliegt bzw. noch herstellbar ist. Auch wenn dies nicht beabsichtigt ist, ist die Erhebung und Speicherung der Daten geeignet, Erkenntnisse zu Leistung oder Verhalten der Beschäftigten zu gewinnen.

VII. Mitarbeiterbefragungen des Betriebsrats

Das gegenüber dem Arbeitgeber bestehende Unterrichtungsrecht des Betriebsrats nach § 80 Abs. 1 Nr. 2 BetrVG schließt nicht aus, dass der Betriebsrat sich auch selbst seine gesetzlichen Aufgaben betreffende Informationen beschafft. Insofern ist auch ihm der Weg der Mitarbeiterbefragung eröffnet.[24]

Keiner Frage bedarf es, dass Auskunftspflichten der Beschäftigten gegenüber dem Betriebsrat nicht bestehen. Die Teilnahme ist freiwillig und muss nach den aufgezeigten Kriterien anonym erfolgen. Eine personenbezogene Erhebung bedarf der Einwilligung, wobei in diesem Falle die Freiwilligkeit nicht in Frage gestellt werden muss.

Prof. Peter Gola
ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. in Bonn.

15 *ULD*, www.datenschutzzentrum.de/wirtschaft/praxis/20070313.htm; *LfD Baden-Württemberg* (o. Fußn. 8), S. 145.
16 Dieser Hinweis hat auf dem Fragebogen selbst und drucktechnisch hervorgehoben zu geschehen, vgl. *LfD Baden-Württemberg* (o. Fußn. 8), S. 138; www.bfdi.bund.de zum Thema Arbeitnehmerdatenschutz/Mitarbeiterbefragungen.
17 Der *HambBfDI* (o. Fußn. 11), Ziff. 5a und b, akzeptiert in diesem Fall die Einwilligung als Erlaubnistatbestand, sofern keine sensiblen, die Persönlichkeit des Befragten betreffenden Daten erfragt werden.
18 So *ULD* (o. Fußn. 15) für den Regelfall.
19 *LfD Baden-Württemberg* (o. Fußn. 8), S. 138.
20 Vgl. *LfD Baden-Württemberg* (o. Fußn. 8), S. 144 f.
21 *BAG* NZA 2001, 167.
22 Zum Begriff und dem Umfang der Mitbestimmung im Einzelnen: *Gola/Wronka* (o. Fußn. 1), Rdnr. 1806 ff.
23 Vgl. *Hessisches LAG* NZA-RR 2002, 200 zur Mitbestimmung bei einer von der Konzernmutter über das Computersystem der Tochter durchgeführten anonymen Befragung.
24 *BAG* BB 1977, 647 = BB 1977, 914.

Mit freundlicher Genehmigung der ZD Redaktion

Runder Tisch zur Datenträger-Archivierung

Im neuen BvD-Ausschuss Datenträger-Archivierung geht es um die Frage der Datenschutzkonformität bei der Archivierung

Vor kurzer Zeit hat der BvD einen neuen Ausschuss initiiert. „Datenträger-Archivierung" heißt er und beschäftigt sich mit der Frage nach der Datenschutzkonformität bei der Archivierung von personenbezogenen Daten. Welche Vorteile das einzelne BvD-Mitglied davon hat, was es mit dem runden Tisch auf sich hat, und wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit den Ausschuss unterstützt, hat BvD-News-Redakteur Michael Braun mit dem stellvertretenden BvD-Vorstandsvorsitzenden Jürgen Hartz und dem Thüringer Landesdatenschützer Dr. Lutz Hasse im Interview diskutiert.

BvD: Der BvD hat einen neuen Ausschuss zur Datenträger-Archivierung (Akteneinlagerung) eingerichtet. Und beteiligt sich an einem „Runden Tisch" zur Datenträger-Archivierung. Wie und wo ist diese Idee entstanden?

Jürgen Hartz: Die Idee entstand spontan während einer unserer Veranstaltungen des BvD mit der Firma Rhenus Office Systems. Während des Vortrags zur neuen DIN der Datenträger-Entsorgung in Berlin wurde in Bezug auf die Erforderlichkeit der Auftragsdatenverarbeitung auch das Thema Akteneinlagerung angesprochen. Dazu berichtete Herr Dr. Hasse von einem ganz aktuellen Datenschutzvorfall bei der Einlagerung von Akten mit personenbezogenen Daten. Ein Foto zeigte eindrucksvoll die brisante Situation der dort gelagerten Akten. Herr Dr. Hasse nannte das dann exemplarisch ein „Datenschutz-Fukushima". Daraus entstand schließlich die Idee für einen „Runden Tisch zur Archivierung" unter Leitung von Herrn Dr. Hasse. Der BvD bringt seine Sachkenntnis und Mitarbeit durch Mitglieder eines neuen Ausschusses ein.

BvD: Ist der Ausdruck „Datenschutz-Fukushima" nicht sehr übertrieben für eine vielleicht etwas unorthodoxe Einlagerung oder ein paar durcheinander gestapelte und umgefallenen Kartons mit Aktenordern?

Dr. Lutz Hasse: Den Ausdruck habe ich geprägt, weil es eben nicht nur um ein paar umgefallene Kartons mit Aktenordnern geht, sondern um ca. 250.000 Aktenordner in z. T. umgestürzten Regalen und Kistenbergen; ein derartiges Chaos habe ich zuvor nicht zu Gesicht bekommen. Gerade in diesem Fall handelt es sich zum Teil auch um besondere personenbezogene Daten im Sinne §3 Abs. 9 BDSG. Da liegen Akten mit Gesundheitsdaten und andere sensible Daten offen und ohne jegliche Kontrolle und Beaufsichtigung herum. Von daher soll der Ausdruck zeigen, dass man Datenträgerarchivierung bzw. Akteneinlagerung nicht auf die leichte Schulter nehmen darf und schon gar nicht einem unzuverlässigen Dienstleister anvertrauen kann. Zwischenzeitlich haben unbefugte Personen in den ungesicherten Räumlichkeiten bereits wohl schon Partys gefeiert. Akten wurden geöffnet und herumgeworfen. Ob dabei auch schon bereits Akten und Unterlagen in fremde Hände gelangt sind und möglicherweise aus den Räumlichkeiten entfernt wurden, konnte bisher nicht festgestellt werden. Nunmehr sind die Räumlichkeiten jedoch gesichert.

BvD: Ist denn durch das BDSG nicht bereits sichergestellt, dass nur zuverlässige Dienstleister derartige Aufgaben übernehmen?

Dr. Lutz Hasse: Der §11 BDSG enthält klare Vorschriften, unter welchen Voraussetzungen ein Auftragnehmer seinen Dienstleister auswählen sollte und welche Maßnahmen er vor der Auftragserteilung und Einlagerung der Akten durchzuführen hat. Wir gehen davon aus, dass dies hier aber nicht erfolgt ist. Im Prinzip kann jeder, der über ein paar Regale und Lagerflächen verfügt, als Dienstleister im Bereich der Archivierung tätig werden. Vermutlich hat auch bei diesem Datenschutz-Vorfall im Rahmen der Angebotsvorbereitung nur der

Im Interview

Foto: Volker Hilscher

Dr. Lutz Hasse
Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Jürgen-Fuchs-Straße 1, 99096 Erfurt
Tel: 0361 . 37719-00
Fax: 0361 . 37719-04
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Jürgen Hartz
Stellvertretender Vorstandsvorsitzender des BvD e.V.

günstigste Preis gezählt. Für die Auswahl eines Dienstleisters bei Datenschutzthemen darf das keinesfalls das wichtigste Kriterium sein. Wir prüfen derzeit, welche Möglichkeiten bestehen, den Auftragnehmer für die Versäumnisse in Anspruch zu nehmen. Hier sind bereits datenschutzrechtliche, aber auch strafrechtliche Maßnahmen eingeleitet.

BvD: Müssen die Auftraggeber jetzt auch mit Kontakt durch Ihre Behörde rechnen?

Dr. Lutz Hasse: Wir prüfen derzeit natürlich auch, ob die Auftraggeber ihre Verpflichtungen zur Kontrolle und ordnungsgemäßem Vertragsabschluss erfüllt haben. Selbstverständlich müssen die Unterlagen schnellstmöglich gesichert, neu eingelagert bzw. an die Auftraggeber zurückgeführt werden. Dabei werden auf jeden Fall Kosten entstehen. Da die Akten weiterhin Eigentum der Auftraggeber sind und diese durch die Einlagerung bei einem Auftragnehmer nicht von ihren originären datenschutzrechtlichen Verpflichtungen befreit sind – was leider kaum bekannt ist –, prüfen wir, wie eine Rückführung und Übernahme der Kosten erfolgen kann.

„Datenschutz-Fukushima" – ein Begriff, den Dr. Lutz Hasse geprägt hat. Dieser liegt nahe, wenn man ein Büro mit einer vollkommen chaotischen Lagerung von Ordnern mit personenbezogenen Daten betritt.

BvD: Wäre für die Auswahl derartiger Dienstleister und Dienstleistungen nicht ein vorheriges Audit beim Auftraggeber hilfreich?

Jürgen Hartz: Zunächst hat der Auftraggeber seinen Dienstleister sogfältig auszuwählen. Dabei kann ein Vor-Ort Besuch hilfreich oder sogar erforderlich sein. Der Datenschutzbeauftragte sollte bei der Auswahl von Dienstleistungen, bei denen personenbezogene Daten betroffen sind, immer eingebunden sein. Im BDSG ist unter §9a schon lange ein Datenschutzaudit festgeschrieben. Danach können Anbieter datenverarbeitender Stellen ihr Datenschutzkonzept sowie die technischen Einrichtungen prüfen und bewerten lassen. Die Ergebnisse können veröffentlicht werden und Auftraggebern eine bessere Einschätzung zur Zuverlässigkeit von Anbietern ermöglichen. Leider gibt es bis heute dieses Gesetz nicht.

BvD: Was hat es mit dem „Runden Tisch" auf sich und wie ist aus diesem Sachverhalt der neue BvD-Ausschuss entstanden?

Jürgen Hartz: Auf seine Ausführungen zu dem Datenschutzvorfall angesprochen, regte Dr. Hasse an, dass es dringend erforderlich wäre, so etwas wie ein Grundlagenpapier, eine Handlungsempfehlung oder Leitlinie zur datenschutzkonformen Einlagerung und Archivierung von Datenträgern zu erstellen. Es bot sich daher an, im BvD einen „Ausschuss Archivierung" zu gründen und den Runden Tisch zu unterstützen.

BvD: Wie wird sich der Runden Tisch zusammensetzen?

Jürgen Hartz: Wir haben vereinbart, dass sich der Runde Tisch aus Herrn Dr. Hasse, den BvD-Ausschussmitgliedern also einem BvD Vorstand und Mitgliedern - vorzugsweise aktive DSB bei Auftraggebern oder Auftragnehmern - zusammensetzt. Darüber hinaus sollen zwei bis vier Vertreter der Wirtschaft, also Anbieter von Archivierungsdienstleistungen eingeladen werden.

BvD: Können bei der Arbeit in BvD-Ausschüssen nur Mitglieder tätig werden und warum sollen Vertreter der Wirtschaft dabei sein?

Jürgen Hartz: Nein, in BvD Ausschüssen können auch Nicht-Mitglieder mitwirken. Jede Person die eine entsprechende Fachkenntnis für die Ziele und Zwecke des Ausschusses mitbringt, kann in den Ausschuss eingeladen werden. Wir planen, in Abstimmung mit Herrn Dr. Hasse, bis Ende Oktober alle Mitglieder des Runden Tisches einzuladen bzw. zu benennen. Vertreter der Dienstleister wollen wir beteiligen, da es wenig sinnvoll ist, Vorgaben und Maßnahmen zu erarbeiten, die in der Realität technisch oder organisatorisch nicht durchführbar sind. Auch Regeln aufzustellen, deren Umsetzung hinterher niemand bezahlen kann oder wird, wäre wenig hilfreich.

BvD: Wann und wo soll denn die Arbeit des Runden Tisches aufgenommen werden und wie wird der weitere Ablauf des Informationsflusses erfolgen?

Dr. Lutz Hasse: Wir haben vereinbart, dass wir zügig Ergebnisse erzielen möchten. Wir wollen keine Gesprächsrunde, die erst nach Jahren etwas vorstellt. Was wir brauchen, sind eine schnelle Arbeitsgrundlage und Dokumentation, mit deren Hilfe Auftraggeber, die eine derartige Dienstleistung benötigen, erkennen, wie sie einen zuverlässigen Auftragnehmer auswählen und worauf sie bei der Vertragsgestaltung achten müssen. Anbieter von Archivierungsservices sollen wissen, dass es nicht ausreicht, ein paar Kartons irgendwo in freie Regale zu stellen. Im Rahmen der Arbeit sollen auch Checklisten entstehen, die beiden Parteien helfen, Mindeststandards für die ordnungsgemäße Auftragsdatenverarbeitung, zur Einlagerung, zur Vertragsgestaltung, aber vor allem zur korrekten Umsetzung der erforderlichen Sicherungsmaßnahmen für personenbezogene Daten auszuarbeiten und umzusetzen. Die erste konstituierende Sitzung des Ausschusses soll möglichst noch im November in den Räumen meiner Behörde stattfinden.

BvD: Wie muss man sich die nächsten Schritte der Arbeit des Ausschusses vorstellen?

Jürgen Hartz: Zunächst findet die konstituierende Sitzung statt. In deren Verlauf legen wir die Ziele und Abläufe sowie eine erste grobe Zeitplanung fest. Der erste Entwurf soll im Düsseldorfer Kreis zur Diskussion gestellt werden. Am Ende stehen die Ergebnisse elektronisch und gedruckt allen Interessenten zur Verfügung.

Dr. Lutz Hasse: Ich bin zuversichtlich, dass der am Runden Tisch versammelte Sachverstand zeitnah einen Orientierungshilfeentwurf zur Diskussion stellen kann, der den Belangen des Datenschutzes, der Auftraggeber und der Auftragnehmer Rechnung trägt.

AK Externe nimmt Datenschutz in Österreich in Augenschein

Referenten gehen ausführlich auf Fragenkatalog der BvD-Mitglieder ein

Salzburg war am 20. und 21. September 2013 das Ziel des Arbeitskreises „Externe Datenschutzbeauftragte“ (AK Externe) im BvD. Zum ersten Mal hat man die deutschen Grenzen überschritten und sich mit Datenschutzgesetz und -organisation unseres Nachbarlandes befasst. Den „Datenschutz in Österreich“ brachte Herr Dr. Gregor König von der österreichischen Datenschutzkommision den 20 Teilnehmern am diesjährigen Herbsttermin spannend und lebhaft nahe. Detailliert wurde am Nachmittag des ersten Tages vom Referenten auch auf einen ausführlichen Fragenkatalog eingegangen, den die deutschen Datenschützer im Vorfeld an Herrn Dr. König übermittelten.

In Österreich ist der Datenschutz anders aufgestellt als bei uns in Deutschland. Den externen Datenschutzbeauftragten gibt es im östlichen Alpenland nicht, wobei aber nicht erst im Zuge der geplanten EU-Datenschutz-Grundverordnung über solche Möglichkeiten nachgedacht wurde. Neben der zentralen Datenschutzkommission gibt es auch noch einen Datenschutzrat aus 30 Mitgliedern, der vornehmlich als Beratungsorgan für die Regierung fungiert und nicht für den Vollzug zuständig ist. Die Datenschutzkommission hat vielfältige Aufgaben, die sich auch im Datensicherheitshandbuch wiederspiegeln. Die letzte Novelle des DSG 2000, des österreichischen Datenschutzgesetzes, gab es 2010, wobei insbesondere die Videoüberwachung konkretisiert wurde. Eine geplante Novelle 2012, in der auch die Möglichkeit der Bestellung eines Datenschutzbeauftragten aufgenommen werden sollte, kam leider über den Planungsstatus nie hinaus. Bereits seit 1980 gibt es das öffentliche Datenverarbeitungsmelderegister DVR, wobei Standardanwendungen nicht meldepflichtig sind und es für definierte Musteranwendungen eine vereinfachte Meldung gibt. Beim Datenexport ins Ausland wird das Genehmigungsverfahren durch die Datenschutzkommission auf Basis einer Angemessenheitsforderung der Datenschutzkommission durchgeführt. Neu war für die deutschen Datenschützer auch die Begrifflichkeit des Informationsverbundsystems, wie sie in § 50 des DSG 2000 näher beschrieben wird. Zusammenfassend

Monika Egle bedankt sich im Namen des AK Externe bei Dr. Gregor König für einen begeisternden und spannenden Vortrag.

Spontanes Gruppenbild mit Dr. Gregor König und weiteren Gästen.

wurde ein gutes Verständnis des Datenschutzgesetzes in Österreich vermittelt, das für den einen oder anderen anwesenden Datenschutzbeauftragten mit österreichischen Niederlassungen oder Gesellschaften deutscher Mutterunternehmen konkrete Ansatzpunkte bietet. Am Ende des spannenden und begeisternd vorgetragenen Vortrages bedankte sich Monika Egle als Mitorganisatorin dieses Treffens im Namen aller Teilnehmer mit einer kleinen Aufmerksamkeit mit dem gemeinsamen Wunsch, dass dies erst der Anfang der geknüpften Kontakte sein soll.

Der auch länderübergreifende Datenschutz in Konzernen war das Schwerpunktthema des weiteren Tagungsverlaufs. Neben der Herausforderung, wie die Rechte der Betroffenen auch in einer komplexen Vertriebsstruktur eines großen Konzerns transparent gewährleistet werden können, wurde auch auf die datenschutzrechtlichen Anforderungen und praktische Umsetzung von Talentmanagement in einem internationalen Konzern detailliert eingegangen. Auch die Mitbestimmung in Konzernstrukturen und die Schnittstellen zum Datenschutz wurden aus Sicht eines Konzernbetriebsrates und eines Konzern-Datenschutzbeauftragten ausführlich vorgestellt.

Den Tagesabschluss bildete eine kurzweilige und lebhafte Stadtführung mit anschließendem gemeinsamen Essen in Europas ältester Gaststätte, dem Stiftskeller St. Peter.

Der Samstagmorgen stand ganz im Zeichen von Auftragsdatenverarbeitung und Übermittlung personenbezogener Daten im Konzern, insbesondere in Drittländer. Auf Basis einer global einheitlichen Datenschutzrichtlinie für den Konzern und der entsprechenden Verfahrensübersichten bzw. Verfahrensverzeichnisse wurde ein Lösungsansatz für ein konzernweites Vertragswerk vorgestellt. Der internationalen Ausrichtung und den dadurch unterschiedlichen Anforderungen (ADV-Vertrag, EU-Standardvertragsklauseln, Funktionsübertragung, Abruf etc.) wird bei diesem Ansatz über verschieden Anlagen Rechnung getragen. Als Folge soll insbesondere der Beitritt neuer rechtlich selbstständiger Konzernorganisationen transparent und strukturiert geregelt und mit überschaubarem Aufwand verbunden sein. Rechtliche Grundlagen für die Übermittlung in Drittländer wurden ebenfalls kompakt zusammengefasst und auf Besonderheiten hingewiesen. Am frühen Nachmittag wurde in Einzelheiten die Datenschutz-Organisation in einer komplexen Konzernstruktur dargestellt und auf zahlreiche spezifische Herausforderungen eingegangen.
Mit einer Feedback-Runde endete traditionsgemäß das Treffen des AK Externe. Viele positive Eindrücke und Erkenntnisse für weitere Impulse wurden mitgenommen. Alle Teilnehmer freuen sich schon auf das nächste Treffen am 7. und 8. März 2014 in Ulm. Nähere Infos für Mitglieder gibt es natürlich zur entsprechenden Zeit auf der BvD-Webseite.

Autor

Manfred Schlitt
AK Externe
E-Mail: ak-externe@bvdnet.de

EU-DSGVO: Was wären die Folgen der Umsetzung?

AK Recht und Praxis[1]: Entwurf mit ungeklärten Fragen

Textverweise

1) Ergebnis eines Impulsvortrages und anschließender Diskussion im Rahmen eines Arbeitstreffens des BvD-Arbeitskreises Recht, TeilnehmerInnen: Norbert Warga, Jochen Brandt, Peter Deckers, Dieter Ehrenschwender, Horst Kübeck, Gerhard Henrikus, Heike Rozek.

2) Ausführlich zur Thematik mit Praxisbeispielen bei Echardt/Kramer/Mester, DuD 2013, Heft 10.

3) KOM (2012) 11 endg. Vom 25.1.2012. Ergänzungen zur polizeilichen und justiziellen Zusammenarbeit finden sich im Entwurf einer Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, s. KOM (2012) endg. vom 25.1.2012. Vollständige Fassung u.a. abrufbar auf der BvD-Linkseite zur BvD-News: https://www.bvdnet.de/bvd-news-links.html

4) Wagner, DuD 2012, 676; Gola/Schulz, RDV 2013, 1; vgl. aber insbesondere zur Kritik, ob Notwendigkeit besteht, den europaweiten Datenschutz in Form einer Verordnung umzusetzen, u.a. Pressemitteilungen unter rsw.beck.de/CMS/?toc=ZD.ARC.201207&docid=335168; http://www.cmshs-bloggt.de/datenschutz/neues-eu-datenschutzpaket-in-der-kritik-subsidiaritatsrugen-in-deutschland-und-frankreich/, jeweils letzter Abruf: 6.10.2013.

5) Vgl. Pkt. 3.2. des Vorschlags, KOM (2012) 11 endg. S. 6.

6) Zum EU-Recht Mester, DuD 2012, 603; zu den Mitgliedstaaten und Bewerberländern siehe außerdem http://europa.eu/about-eu/countries/index_de.htm, letzter Abruf 8.6.2012; Zu den Aufgaben der Kommission vgl. http://europa.eu/about-eu/institutions-bodies/european-commission/index_de.htm, letzter Abruf: 12.2.2013.

Inzwischen dürften auch diejenigen, die sich nur wenig für den Datenschutz interessieren, damit konfrontiert worden sein, dass seit 2012 eine europaweite Regelung des Datenschutzes geplant ist. Das ist nicht zuletzt ein Ergebnis zahlreicher Berichte in der Tagespresse zu „Datenschutzpannen“ (PRISM, XKeyscore und TEMPORA seien in diesem Zusammenhang nur beispielhaft genannt). Mit vermehrter Häufung von internationalen Datenschutzproblemen steigern sich auch die Fragen – oder auch der Ruf – nach internationalen Regelungen und wird damit u.a. der bereits vorliegende Entwurf der EU-Kommission für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 25.01.2012 (EU-DSGVO[2]) in den Fokus rechtlicher Auseinandersetzungen gebracht.[3] Während jedoch die einen noch über den Sinn und Unsinn einzelner Regelungen bzw. sogar über Formulierungen diskutieren, zweifeln andere gleich prinzipiell die Notwendigkeit europaweiter Vorschriften an.[4] Doch worauf ist eigentlich diese generelle Abneigung gegen eine europaweite Regelung zurückzuführen?

Wird das zunächst von der EU-Kommission verfolgte Ziel einer Vereinheitlichung des Datenschutzniveaus in der EU, einer weitgehenden Reduzierung des Verwaltungsaufwands für die Beteiligten und der Verbesserung der Durchsetzung von Rechten Betroffener sowie einer wirksamen länderübergreifenden Überwachung des Datenschutzes[5] betrachtet, so lässt sich daran zunächst einmal nichts Kritikwürdiges feststellen. Zahlreiche ungelöste Datenschutzfragen im Bereich international tätiger Unternehmen ließen sich vielmehr leichter lösen. So ist es nicht überraschend, dass Stimmen laut werden, die eine zeitnahe Umsetzung der EU-DSGVO vehement fordern. Doch wie so häufig, ist die Lösung nicht so einfach. Genauso viele Gründe, die für die EU-DSGVO sprechen, können auch gegen sie aufgeführt werden. Eine der grundlegendsten ungeklärten Fragen ist: Muss es eigentlich eine Verordnung sein, die die bisherige Regelung durch eine Datenschutz-Richtlinie ablöst?

Hintergründe

Zu berücksichtigen ist, dass nach dem derzeit vorliegenden Entwurf einer Verordnung diese für alle zur Zeit der Europäischen Union (EU) angehörenden 28 Mitgliedstaaten verbindlich gelten soll. Vorgelegt wurde der Entwurf der EU-DSGVO durch die Europäische Kommission (EU-Kommission), die gemeinsam mit dem Europäischen Parlament und dem Rat der Europäischen Union im Rahmen eines ordentlichen Gesetzgebungsverfahrens die Rechtsetzungsgewalt der Europäischen Union darstellt.[6] Ihren Gesetzgebungsvorschlag zum vorliegenden Entwurf einer EU-DSGVO stützt die EU-Kommission auf Art. 16 Abs. 2 des Vertrages über die Arbeitsweise der europäischen Union (AEUV). Danach kann und darf die EU Vorschriften zunächst einmal zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionrechts fallen, sowie des freien Datenverkehrs erlassen.[7] Eine Regelung des europäischen Datenschutzrechts gibt es auch schon jetzt, nämlich durch die Richtlinie 95/46/EG (Datenschutzrichtlinie), deren Vorgaben durch die jeweiligen Mitgliedstaaten auf nationaler Ebene umzusetzen sind.

Datenschutzrecht im Wege der EU-Verordnung

Wurde also das europäische Datenschutzrecht bisher durch eine Richtlinie geregelt, handelt es sich bei dem vorliegenden Entwurf um eine Verordnung. Vielen sind die sich daraus für die einzelnen Länder ergebenden Konsequenzen aber gar nicht bewusst bzw. mangels europarechtlicher Kenntnisse vielleicht auch einfach nicht bekannt. Während eine Richtlinie einer Umsetzung in den einzelnen Mitgliedstaaten bedarf, wirkt

die Verordnung in den jeweiligen Mitgliedstaaten der Europäischen Union nach ihrem Inkrafttreten unmittelbar und bedarf keinerlei Tätigwerden der einzelnen Staaten (vgl. Art. 288 AEUV). Damit richten sich die geplanten Vorgaben des vorliegenden Entwurfes einer EU-DSGVO nicht mehr nur an die Mitgliedstaaten selbst, mit der Verpflichtung bestimmte Vorgaben umzusetzen, sondern auch direkt an deren nach innerstaatlichem Recht zuständigen Organe sowie deren Glieder (bspw. Behörden, Gerichte), die damit unmittelbar verpflichtet sind, die sich aus der EU-DSGVO ergebenden Rechte und Pflichten umzusetzen bzw. zu berücksichtigen.[8] Damit bedarf es gerade keiner weiteren nationalen Rechtsakte mehr, um innerstaatlich eine unmittelbare Wirkung europäischer Regelungen zu entfalten.

Teilweise findet sich immer noch die Überzeugung, dass notfalls weiterhin nationale Regelungen zum Datenschutz problemlos erlassen werden könnten. Den Mitgliedstaaten ist jedoch bei einer europäischen Verordnung eine Modifikation vorhandener Regelungen untersagt („Umsetzungsverbot").[9] Es kann nach Art. 290 Abs. 1 AEUV der EU-Kommission aber bspw. die Befugnis übertragen werden, sog. delegierte Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften zu erlassen. Außerdem besteht nach Art. 291 Abs. 2 AEUV die Möglichkeit, detaillierte Maßnahmen zur Umsetzung europäischer Rechtsakte vorzugeben (Durchführungsrechtsakte).[10] Das bedeutet zunächst einmal, dass die EU-Verordnung in ihrem Anwendungsbereich eine abschließende Regelung ist, sofern keine expliziten Öffnungen für nationale Regelungskompetenzen mit aufgenommen wurden.

Fazit

Sicherlich kann der vorgelegte Entwurf einer EU-DSGVO bei der Bewertung zahlreicher internationaler Datenschutzprobleme viele noch offene Fragen beantworten bzw. für die Zukunft regeln. Die Kritik an der EU-DSGVO ist aber nicht rein akademischer Art. Fakt ist nämlich, dass es im Entwurf noch zahlreiche ungeklärte Fragen gibt, weil sich die Beantwortung bspw. noch nach den zukünftigen Entscheidungen der EU-Kommission richten soll (dort wo sich die EU-Kommission die

Der aktuelle Entwurf der EU-DSGVO wird ausgiebig diskutiert, wie hier in Brüssel beim Informationstag des BvD im Jahr 2012.

Regelung vorbehalten hat) bzw. unbestimmte Rechtsbegriffe nicht ausreichend definiert sind.[11] Dabei gilt, dass anders als oftmals gedacht, eben bei fehlender oder nicht ausreichender Regelung, nicht einfach auf bereits bestehende oder noch zu schaffende nationale Spezialregelungen zurückgegriffen werden kann. Vielmehr ist es wichtig zu erkennen, dass bei allen Vorteilen einer einheitlich europaweiten Regelung des Datenschutzes diese entweder wirklich so konkret sein muss, dass alle wesentlichen Punkte abschließend geklärt und somit Rechtsicherheit erreicht ist oder aber doch noch die Umsetzung im Rahmen einer Richtlinie erfolgt.[12] Denn auch eine Richtlinie kann durchaus Vorschriften enthalten, von denen der nationale Gesetzgeber nicht abweichen darf. Es bleibt dann weiterhin dem nationalen Gesetzgeber überlassen, eine entsprechende Regelung mit einem der Richtlinie entsprechenden Inhalt zu schaffen. Er darf die Regelung dabei aber weder laxer noch strenger ausgestalten (Stichwort „Vollharmonisierung").[13] Daher müssen auch bei Vorliegen einer Richtlinie geplante nationale Bestimmungen die europäisch gesetzten Grenzen berücksichtigen. So dass auch durch eine überarbeitete Richtlinie die Möglichkeit der Vereinheitlichung des Datenschutzniveaus zu erreichen wäre.

Textverweise

7) Vgl. KOM (2012) 11 endg., Ziff. 31 der Begründung; zu der Entwicklung der Kompetenz der EU-Kommission nach Art. 16 siehe bei Streinz, DuD 2011, 602, S. 603 f.
8) Vgl. hierzu insgesamt bei Nettesheim, a.a.O., Art. 288 Rn. 98; vertiefend auch Streinz, Europarecht, 9. Aufl., Heidelberg 2012.
9) Vgl. Gola/Schulz, RDV 2013, 1, S.2.
10) Zur Kritik bei Gola/Schulz, RDV 2013, 1, S.2; Gola, EuZW 2012, 332.
11) Zu den zahlreichen Kritikpunkten bspw. bei Wagner, DuD 2012, 676; Gola/Schulz, RDV 2013, 1 m.w.Nw.; Härting, BB 2012, 459; Gola, EuZW 2012, 332; Stellungnahme des BvD, Positionspapier zur EU-DSGVO, abrufbar unter https://bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/Standpunkte/121018-BvD-EU-DSGVO-E-Positionspaper_FINAL.pdf , letzter Abruf am 16.8.2013; Stellungnahme der GDD hinsichtlich der Auswirkungen auf die Privatwirtschaft; I.2, abrufbar unter: http://www.gdd.de/aktuelles/news/gdd-stellungnahme-zu-den-grundsatzen-des-vorschlages-der-europaischen-kommission-einer-datenschutz-grundverordnung, letzter Abruf: 6.10.2013 oder auch mit Beispielen bei Eckhardt/Kramer/Mester, DuD 2013, Heft 10; Eckhardt/Kramer, DuD 2013, 287.
12) Es sind sowohl eine Richtlinie als auch Beschlüsse, Empfehlungen sowie Stellungnahmen denkbar (vgl. Art. 288 AEUV) (Vgl. Nettesheim, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Losebl., Stand 2012, Art. 288 Rn. 86 f.).
13) EuGH v. 24.11.2011 –Rs. C-468/10, Rs. C 469/10 – ASNEF/FECEMD-Rz. 35; gilt auch bei anderen europarechtlichen Richtlinien, vgl. bspw. zur Verbraucherkreditrichtlinie das EuGH Urteil vom 12.7.2012 - C-602/10; mit Anm. Möller, LMK 2012, 337364.
14) Dazu näher bei Streinz, DuD 2011, 602, S. 605.

Autorin

Dr. Britta Alexandra Mester
CvO Universität Oldenburg, Mitherausgeberin Datenschutz und Datensicherheit, Fachausschussleiterin DGRI Arbeitsrecht, Externe Datenschutzbeauftragte

Aus der Geschäftsstelle

(Foto: Christina Kurby)

Erweiterung der Geschäftsstelle

Nachdem die BvD-Geschäftsstelle inzwischen mit sehr vielen Aufgaben betraut ist hat der Vorstand bereits auf der Mitgliederversammlung im April 2013 die Erweiterung der Geschäftsstelle angekündigt. Seit dem 15. September 2013 ist nun Frau Claudia Melcher mit an Bord. Die Diplom-Politologin hat langjährige Erfahrung in der Verbandsarbeit durch ihre Tätigkeit in diversen großen Verbandsorganisationen. Insbesondere kennt sie sich in der Bearbeitung politischer Themen und der Zusammenarbeit der verschiedenen Stakeholder aus und wird den Vorstand hier zukünftig unterstützen. Die weiteren Schwerpunkte ihrer Tätigkeit im BvD sind die Leitung und Betreuung der Geschäftsstelle und gerade in der Anfangszeit die intensive Betreuung der DSZ - Datenschutz Zertifizierungsgesellschaft mbH in Berlin und die dazu erforderliche Abstimmung mit der GDD.
Wir freuen uns auf die Zusammenarbeit und wünschen Frau Melcher zum Start alles Gute!

Der BvD in Zahlen

852 Mitglieder
303 Firmenmitglieder
120 registrierte externe Datenschutzbeauftragte
219 freiwillige Selbstverpflichtungen auf das „berufliche Leitbild des Datenschutzbeauftragten“
(Stand September 2013)

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

Nächste Seminare der udis

Alle Termine der kommenden Wochen kompakt auf einen Blick

Die Ulmer Gesellschaft für Datenschutz und IT-Sicherheit hat die Termine für ihre nächsten Seminare veröffentlicht. Aus der nachfolgenden Aufstellung können Sie sich einen Überblick über die nächsten Weiterbildungen verschaffen. BvD-Seminare finden Sie auf der Folgeseite.

Grundlagen der EDV für Datenschutzbeauftragte
22.10.2013-23.10.2013

Ausbildung zu zertifizierten fachkundigen Datenschutzbeauftragten nach dem Ulmer Modell
23.09.2013-28.09.2013 (1. Woche)
21.10.2013-26.10.2013 (2. Woche)
11.11.2013-15.11.2013 (3. Woche)

Ausbildung zu zertifizierten fachkundigen Datenschutzbeauftragten nach dem Ulmer Modell
04.11.2013-09.11.2013 (1. Woche)
02.12.2013-07.12.2013 (2. Woche)
13.01.2014-17.01.2014 (3. Woche)

Ausbildung zum fachkundigen IT-Sicherheitsbeauftragten
21.10.2013-26.10.2013 Ulmer Woche
11.11.2013-16.11.2013 Regensburger Woche
02.12.2013-06.12.2013 Hamburger Woche

Wie prüfe ich meinen Auftragsdatenverarbeiter? Effiziente Prüfungssystematik von Auftragnehmern im Rahmen der Auftragsdatenverarbeitung
18.11.2013-19.11.2013

Datenschutzpraxis - hautnah
14.10.2013-18.10.2013 – Workshop an fünf Tagen in drei Blöcken. Die drei Blöcke können jeweils auch einzeln gebucht werden:

Block 1 (14.10.2013): Grundlagen des Datenschutzrechts
Block 2 (15.10.-17.10.2013): Professionelle Strategien der Datenschutzpraxis
Block 3 (18.10.2013): Entwicklung eines Datenschutzkonzepts anhand des BSI-Grundschutz-Handbuchs

Betriebswirtschaft für Datenschutzbeauftragte
15.01.2014

ISO 27001-Zertifizierung auf Basis von IT-Grundschutz – Kein Problem?!
03.02.2014-04.02.2014
Seminarort für das ISO-Seminar ist in Hamburg.

Das udis-Team von Prof. Dr. Gerhard Kongehl bietet in den nächsten Wochen interessante Seminare zum Thema Datenschutz an.

Seminare und Treffpunkte für BvD-Mitglieder

Aktuelle Termine der Regionalgruppen und Seminarveranstalter

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-Webseite https://www.bvdnet.de möglich. Das gilt auch für die angebotenen Seminare des BvD.

Treffen der Regionalgruppen und Arbeitskreise

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

RG Südwest Treffen Mainz
18.10.2013 16:00 Uhr - 19:00 Uhr

RG Bayern Treffen Unterschleißheim
25.10.2013 13:00 Uhr - 18:00 Uhr

RG Nord Treffen
31.10.2013 14:00 Uhr - 19:00 Uhr

RG Südwest Treffen Alsenborn
12.12.2013 16:00 Uhr - 19:00 Uhr

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

RG Mitte Treffen Hungen
23.01.2014 17:30 Uhr - 21:30 Uhr

RG Südwest Treffen
14.03.2014 16:00 Uhr - 19:00 Uhr

RG Süd Treffen Ulm
14.03.2014 10:00 Uhr - 17:00 Uhr

RG Süd Treffen Ulm
27.06.2014 10:00 Uhr - 10:30 Uhr

AK Sozial Treffen in Frankfurt
18.10.2013 09:30 Uhr - 17:00 Uhr

Seminare des BvD

Sonderseminar - Datenschutzunterweisungen & Auftragsdatenverarbeitung
16.10.2013 09:30 Uhr - 17:30 Uhr
Stefan Purder, Konzern-DSB, Xella International GmbH
Zweiteiliges Seminar. Praxisveranstaltung besonders für neu bestellte DSB.
Teil 1: Wie man interessante Datenschutz-Schulungen und Unterweisungen gestaltet und durchführt und die gesetzlichen Verpflichtungen vornimmt. Teil 2: Umsetzung der Vorgaben zu §11 und §9 Anlage im Rahmen der ADV mit internen und externen Dienstleistern.

ausgebucht - Sonderseminar - Internationaler Datentransfer
16.10.2013 09:30 Uhr - 17:30 Uhr

Sonderseminar - Praxisworkshop Datensicherheit und IT-Wissen für den DSB
16.10.2013 09:30 Uhr - 17:30 Uhr
Andreas Hessel, langjähriger betrieblicher DSB und IT-Sicherheitsbeauftragter
Das Seminar eignet sich besonders für jene DSB, die sich mit IT-Grundlagen und Datensicherheit beschäftigen wollen.

Seminar - Videoüberwachung - als udis-refresher Seminar anerkannt
5.11.2013 09:30 Uhr - 17:30 Uhr
Dr. Stefan Brink, Leiter Datenschutz in der Privatwirtschaft, beim Landesbeauftragten für den Datenschutz Rheinland-Pfalz, Thomas Spaeing, BvD-Vorstandsvorsitzender, Jürgen Hartz, stellvertretender BvD-Vorstandsvorsitzender
Das Seminar vermittelt die Grundlagen der Techniken zur Videoüberwachung und zeigt den Einsatz in Bezug auf die gesetzlichen Forderungen des BDSG.

BvD-Datenschutztage 2014

Wettbewerbsfaktor Datenschutz!

21. und 22. Mai 2014 in Berlin

Deutschland Land der Ideen
Ausgewählter Ort 2011

BvD e.V.
Die Datenschützer

- 2 Tage intensives Netzwerken und anregender Gedankenaustausch mit fachkundigen Teilnehmern, Referenten und Vertretern von Aufsichtsbehörden
- Herausragende Keyspeaker
- 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 99,00 Euro incl. Frühstück, DZ 120,00 Euro incl. Frühstück. Bitte buchen Sie direkt beim **NH-Berlin Mitte,** Stichwort „BvD VT 2014“, gültig bis 15.12.2013.

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: 21. und 22. Mai 2014!

BvD-Datenschutz-Symposium 2013

mit Sonderseminaren

16. und 17. Oktober 2013
in Frankfurt / Main

- BvD stellt neues Datenschutzaudit vor
- Austausch mit Experten und Fachleuten zum Berufsbild des Datenschutzbeauftragten
- Herausragende Keyspeaker und Fachreferenten: Deutsche Telekom AG, Nestlé Deutschland AG, DB Mobility Logistics AG, LfD Schleswig-Holstein
- Sonderseminare zur Fortbildung (s.u.)

Für weitere Infos QR-Code mit dem Smartphone scannen:

Jetzt online zum BvD-Datenschutz-Symposium anmelden*: www.bvdnet.de oder per FAX: 030 . 21 96 43 92

Sonderseminar zum Symposium: Datenschutzunterweisungen und Auftragsdatenverarbeitung

Referent: Stefan Purder

Das Seminar hilft, erste wichtige Aufgaben im Unternehmen als interner oder externer Datenschutzbeauftragter vorzubereiten. Insbesondere die Akzeptanz bei Mitarbeitern und spätere Kommunikation kann durch interessante und fachkundige Unterweisung und Schulungen im Rahmen der Datenschutzverpflichtungen erreicht werden. Im zweiten Teil des Seminars erfahren Sie wichtige Grundlagen und Umsetzungsvorschläge zu den Vorschriften zur Auftragsdatenverarbeitung. Wir zeigen Ihnen, wie Sie diesen Bereich der Datenschutzarbeit umsetzen und welchen Nutzen Sie und Ihr Unternehmen daraus ziehen können. Im Seminar enthalten: CD mit Mustern für Unterweisung und Grundlagenschulung (BWRmedia Autor: S. Purder)

Datum: 16.10.2013, Ort: Frankfurt - NH Hotel Frankfurt City*

Sonderseminar zum Symposium: Praxisworkshop Datensicherheit und IT-Wissen für den DSB

Referent: Andreas Hessel

Informationen zum Workshop: Dieser Praxisworkshop zeigt, welche Gefährdungen analysiert und welche gesetzlichen Anforderungen beachtet werden müssen und beschreibt Wege zur datenschutzkonformen Einbindung mobiler privater Endgeräte in die Unternehmens-IT. Verfügbare Lösungen werden vorgestellt und Strategien für den Betrieb erarbeitet und Musterregelungen besprochen. Im Seminar enthalten: CD „Datensicherheit in der Praxis“ (BWRmedia Autor: A. Hessel)

Datum: 16.10.2013, Ort: Frankfurt - NH Hotel Frankfurt City*

Tipp: Buchen Sie ein Sonderseminar zusammen mit dem BvD Datenschutz-Symposium und sparen Sie 50,00 €.

*Teilnahmegebühr am BvD-Datenschutz-Symposium: 250,00 Euro für BvD-Mitglieder, 350,00 Euro für Nicht-Mitglieder; Teilnahmegebühr an einem Sonderseminar: 399,00 Euro

Ansprechpartner

BvD-Geschäftsstelle
Budapester Straße 31
10787 Berlin
Tel.: +49 30 21964397
E-Mail: bvd-gs@bvdnet.de
Web: https://www.bvdnet.de

Der BvD in Zahlen

- gegründet 1989
- 852 Mitglieder insgesamt (Sep. 2013)
- 303 Firmenmitglieder
- 120 registrierte externe Datenschutzbeauftragte (Sep. 2013)
- 219 freiwillige Selbstverpflichtungen auf das „berufliche Leitbild des Datenschutzbeauftragten“
- über 100 Vermittlungsanfragen jährlich
- zahlreiche Regionalgruppen bundesweit (zurzeit Baden, Bayern, Mitte, Nord, Ost, Süd, Südwest, West)
- Arbeitskreise zu den Themen: externe Datenschutzbeauftragte, Medizin, Recht & Praxis, Schule, Datenschutz in sozialen Einrichtungen, Social Media