BvD

Die Datenschützer

BvD-News

Mitgliederzeitung
August 2005

Themen: Ausstattung des Datenschutzbeauftragten +++ Datenschutz in Anwaltskanzleien +++ Videokennzeichen +++ Spam +++ Veranstaltungsberichte +++

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

BvD-News, Mitgliederzeitung August 2005

Der Datenschutzbeauftrage

Technik: Video und Spam

Veranstaltungsberichte

Der Verband

• • • • • Editorial • • • • •

Liebe Mitglieder,

der Schwerpunkt dieser „BvD-News" liegt in der Berichterstattung aus den BvD-Arbeitskreisen. Im BvD sind momentan drei Arbeitskreise tätig:

Der Arbeitskreis „Die zukünftige Entwicklung des Datenschutzrechts in Deutschland" (kurz: AK Datenschutzrecht) widmet sich schon seit vielen Jahren sowohl aktuellen Gesetzesinitiativen als auch anderen aktuellen Themen. In dieser Ausgabe der „BvD-News" können Sie eine Stellungnahme des AK zur Videoüberwachung und ein Arbeitspapier zur Spam-Behandlung lesen.

Der Arbeitskreis „Externe Datenschutzbeauftragte" dient als Plattform für den Erfahrungsaustausch zwischen externen Datenschutzbeauftragten und will Handlungshilfen, Musterverträge und Standards für die Tätigkeit und Qualifikation des externen Datenschutzbeauftragten erarbeiten. Lesen Sie hierzu einen Bericht über die Arbeit des AK Externe von Albert Neuner.

Der Arbeitskreis „Ausstattung des Datenschutzbeauftragten" möchte Hinweise zur technischen und finanziellen Ausstattung von Datenschutzbeauftragten geben. Im letzten halben Jahr wurde eine Umfrage zum Ist-Zustand durchgeführt, die momentan ausgewertet wird. In diesem Heft lesen Sie einen Beitrag von der Leiterin des AK, Ingrid Pahlen-Brandt, zum Stellenwert und der Eingruppierung der Stelle des Datenschutzbeauftragten.

Im Vorstand hat es wieder einige Veränderungen gegeben. Peter Kaiser (Beisitzer) ist aus beruflichen Gründen im Spätsommer 2004 aus dem Vorstand ausgeschieden. Peter Kaiser war auch viele Jahre Mitglied im AK Datenschutzrecht. Der Vorstand bedankt sich herzlich bei ihm für die von ihm geleistete Arbeit! Nach Ausscheiden des bisherigen Justiziars Dr. Bergmann nimmt seit April 2004 Uwe Meister zusätzlich die Aufgaben des Justiziars wahr.

Auf eine bedenkliche Entwicklung möchte ich hier noch besonders hinweisen. Immer wieder erreichen den BvD Hinweise auf Angebote externer Datenschutzbeauftragter, die Ihre Dienstleistungen zu Dumping-Preisen anbieten. Im krassesten Fall bot ein externer Datenschutzbeauftragter für eine Arztpraxis seine Dienste für 2 EUR pro Monat an. Für einen solchen Preis kann niemand fachgerechten Datenschutz besorgen. Der BvD wird vehement versuchen, derartige Fehlentwicklungen zu stoppen! Sollten Sie von solchen Angeboten wissen, teilen Sie es uns bitte mit, damit wir etwas dagegen unternehmen können.

Ich wünsche Ihnen einen schönen Sommer!

Ihr Hannes Federrath

Zum Stellenwert und der Eingruppierung der Stelle des Datenschutzbeauftragten

Die Anforderungen an Art, Umfang und Tiefe der erforderlichen Fachkunde erfordern Experten auf drei Gebieten: Recht, Technik, Wirtschaft. Um Mitarbeiter mit diesen Voraussetzungen finden und dauerhaft im Unternehmen halten zu können, ist es erforderlich, ihnen auch eine entsprechende Eingruppierung sowie Ausstattung am Arbeitsplatz zu bieten.

Von Ingrid Pahlen-Brandt

Ausgangslage

Ausgangspunkt für die Bewertung ist die Beschreibung des Amtes des Datenschutzbeauftragten im Gesetz. Soweit bei der Stellenbewertung an Arbeitsvorgänge anzuknüpfen ist, also an Arbeitsleistungen, die bezogen auf den Aufgabenbereich des Stelleninhabers zu einem bei natürlicher Betrachtung abgrenzbaren Arbeitsergebnis führen – wie etwa im Geltungsbereich des BAT – ist die gesamte Tätigkeit des Datenschutzbeauftragten als ein Arbeitsvorgang anzusehen, denn die gesamte Tätigkeit ist ausgerichtet auf die Gewährleistung des informationellen Selbstbestimmungsrechts bei der Verarbeitung personenbezogener Daten im Rahmen ihres Zuständigkeitsbereiches. Der nicht aufteilbare Aufgabenkreis ist nur einer einheitlichen rechtlichen Bewertung zugänglich. (vgl. BAG AP Nr. 205 zu §§ 22, 23 BAT 1975 zu Gleichstellungsbeauftragten).

Fachkunde

Zur Erfüllung der vom Datenschutzbeauftragten geforderten Fachkunde werden insbesondere juristische, technische und betriebswirtschaftliche Kenntnisse benötigt. Für den erforderlichen Umfang und die erforderliche Tiefe der Kenntnisse sind die Größe und die Komplexität der von vom Datenschutzbeauftragten zu betreuenden Organisation (Behörde oder Betrieb) mitbestimmend. Die im Folgenden beschriebenen Anforderungen sind typisch für viele Organisationen (vgl. zur Fachkunde ausführlich Simitis u.a., Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, Rdnr 83 ff.).

- **Juristische Kenntnisse:** Das Datenschutzrecht ist ein Querschnittsgebiet und eine junge Rechtsmaterie mit noch vielen ungeklärten Fragen und ungewöhnlich vielen Generalklauseln. Für die korrekte Anwendung des Rechtes ist dessen vertieftes Verständnis erforderlich, das regelmäßig durch ein juristisches Studium erlangt werden kann.
- **Technische Kenntnisse:** Erforderlich sind neben grundlegenden IT-Kenntnissen nachgewiesene Spezialkenntnisse zur IT-Sicherheit.
- **Betriebswirtschaftliche Kenntnisse:** Datenschutzbeauftragte müssen nicht nur die bestehenden organisatorischen Abläufe kennen. Sie müssen bei der Beratung im Vorfeld und bei der Einführung neuer Verfahren – dies ist ein Schwerpunkt ihrer Tätigkeit – in der Lage sein, Hindernisse zu erkennen und Vorschläge zu deren Abhilfe zu erarbeiten und zu unterbreiten.

Verantwortung (Zuverlässigkeit)

Charakteristisch für den Datenschutzbeauftragten ist, dass ihm aufgrund seiner Funktion aus dem Gesetz nicht das Recht zusteht, Anordnungen zu

treffen. Der Datenschutzbeauftragte kann lediglich Feststellungen treffen und Vorschläge zur Verbesserung des Datenschutzes vorlegen. Gleichzeitig ist er jedoch auch weisungsfrei.
Aus dem Fehlen einer gesetzlich verankerten Anordnungsbefugnis und dem Fehlen wirksamer Einwirkungsbefugnisse ist jedoch nicht auf fehlende Verantwortung des Datenschutzbeauftragten zu schließen. Diese Annahme widerspräche dem erkennbaren Willen des Gesetzgebers, dessen Regelungsziel es ist, durch Datenschutzbeauftragte das informationelle Selbstbestimmungsrecht der von der Datenverarbeitung Betroffenen zu sichern.
Die Tätigkeit eines Arztes zeichnet sich durch ein hohes Maß an Verantwortung aus, obwohl die Entscheidung über das Annehmen oder Verwerfen des Therapievorschlages allein dem Patienten obliegt. Nicht anders ist es mit „Diagnose und Therapie" des Datenschutzbeauftragten. Dem Leiter der Daten verarbeitenden Stelle bleibt es überlassen, sie zu akzeptieren. Kommt dieser zu einer Fehlentscheidung, ist der Datenschutzbeauftragte verpflichtet, die Kontrollstelle einzuschalten, die mit wirksamen Einwirkungsbefugnissen für datenschutzgemäße Verhältnisse sorgen kann. (zum Arztbeispiel siehe Klaus Krasemann, Das Eingruppierungsrecht des Bundes-Angestelltentarifvertrages (BAT), 5. Aufl. Frankfurt am Main, Rdnr. 517 unter Bezugnahme auf BAG AP Nr. 116 zu §§ 22, 23 BAT 1975)
Das Maß seiner Verantwortung richtet sich nach dem Schutzbedarf der in der Organisation verarbeiteten personenbezogenen Daten und der Anzahl der hiervon Betroffenen.

Eingruppierung/Vergleichbare Stellen

Die Betrachtung der Regelungen

- zur Weisungsfreiheit (§ 4f Abs. 3 S. 2 BDSG),
- die Vorgabe zur Unterstellung (§ 4f Abs. 3 S. 1 BDSG),
- das Unterstützungsgebot (§ 4f Abs. 3 S. BDSG) und
- das Benachteiligungsverbot (§ 4f Abs. 5 BDSG)

ergibt, mit welchen Stellen innerhalb der Organisation die Stelle des Datenschutzbeauftragten gleichzustellen ist.

Weisungsfreiheit

Der Datenschutzbeauftragte ist bei der Anwendung seiner Fachkunde auf dem Gebiete des Datenschutzes weisungsfrei (§ 4f Abs. 3 S.1 BDSG). Diese Unabhängigkeit zeichnet seine Tätigkeit gegenüber nahezu allen Arbeitnehmern aus, die dem Direktionsrecht von Vorgesetzten unterstehen.

Unterstellung unter die Geschäftsleitung

Durch die unmittelbare Unterstellung des Datenschutzbeauftragten unter die Geschäftsleitung (§ 4f Abs. 3 S. 1 BDSG) räumt das Gesetz Kompetenz- und Kommunikationsschwierigkeiten aus dem Weg und ermöglicht es, Datenschutzfragen unmittelbar in den Entscheidungsprozess über Struktur und Aktivitäten der verantwortlichen Stelle einzubringen.

Unterstützungsgebot

Die Daten verarbeitenden Stellen haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgabe zu unterstützen (§ 4f Abs. 5 S.1 BDSG). Die Unterstützungspflicht verlangt eine Bewertung, die es ihm ermöglicht, mit den für ihn relevanten Akteuren im Betrieb auf gleicher Augenhöhe zu verhandeln.
Unterstützung erhält der Datenschutzbeauftragte insbesondere auch durch klare Aussagen zum Stellenwert des Datenschutzes im Leitbild der Organisation. Somit wird für die einzelnen Struktureinheiten (Unternehmensbereiche, Abteilungen etc.) deutlich, dass der Datenschutzbeauftragte bei allen Fragen der Verarbeitung personenbezogener Daten mit einzubeziehen ist.

Benachteiligungsverbot

Datenschutzbeauftragte dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden (§ 4f Abs. 3 S.3 BDSG). Dies betrifft insbesondere auch ihre sachliche und personelle Ausstattung sowie die tarifmäßige Eingruppierung.

Gleiche Augenhöhe

Eine Orientierung bezüglich der Eingruppierung des Datenschutzbeauftragten stellen diejenigen Mitarbeiter dar, mit denen sich der Leiter der Organisation regelmäßig auseinandersetzt, um die für das Unternehmen wichtigen Entscheidungen zu erörtern.

Häufig wird daran gedacht, die Funktion des Datenschutzbeauftragten dem Leiter von Abteilungen zusätzlich zu übertragen, etwa dem Leiter der Personalabteilung, der IT-Abteilung, des Controlling oder des Vertriebs. Die Bestellung dieser Funktionsträger scheitert allerdings an deren Zuverlässigkeit, die aufgrund möglicher Interessenskonflikte nicht angenommen werden kann.

Die Orientierung an diesen Stellen bei der Eingruppierung wird jedoch regelmäßig zu einer zutreffenden Stellenbewertung führen, die mit den oben genannten Punkten übereinstimmen wird.

Zusammenfassung

Personen, die den Anforderungen an die Fachkunde auf juristischem, technischem und wirtschaftlichem Gebiet voll gerecht werden, wird es selten geben. In der Praxis reicht es aus, dass ein Fachmann auf einem der Gebiete die Beurteilungen von Fachleuten zu den anderen Gebieten selbständig einzuschätzen vermag. Ob der Datenschutzbeauftragte Informatiker, Jurist oder Betriebswirt sein soll, entscheidet nicht das Gesetz. Das Gesetz fordert lediglich, dass alle drei Komponenten in ausreichendem Maße gegeben sind. Bei den meisten Betrieben bzw. Behörden wird die Arbeit ohne eine abgeschlossene Hochschulausbildung oder eine entsprechende qualitätsgesicherte Zusatzausbildung nicht bewältigt werden können.

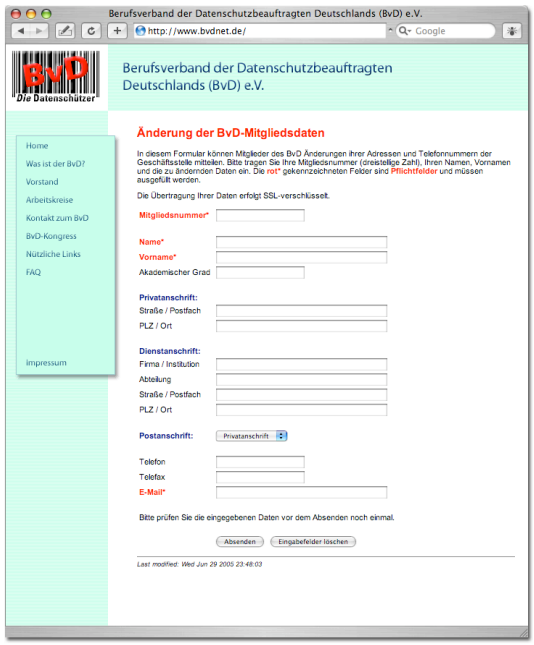
Als Richtwerte für die Qualifikation und Eingruppierung von Datenschutzbeauftragten können andere leitende Positionen wie IT-Leiter oder Personalleiter dienen. Darüber hinaus sollte der Datenschutz als wichtiges Ziel in der Unternehmenskultur verankert sein. Eine derartige Vorgehensweise hilft nicht nur die gesetzlichen Auflagen zu erfüllen, sondern erlaubt darüber hinaus auch die Vermarktung des Datenschutzes durch die Organisation und wird somit zu einem Wettbewerbsvorteil.

• • • • • Service • • • • •

E-Mail-Adresse und Stammdaten übers Web aktualisieren

Unter http://www.bvdnet.de können Sie der Geschäftsstelle Ihre E-Mail-Adresse mitteilen. Es lohnt sich, wenn Sie uns Ihre E-Mail-Adresse mitteilen. Aktuelle Informationen der Geschäftsstelle – beispielsweise zu vergünstigten Konditionen für die Teilnahme an bestimmten Weiterbildungsveranstaltungen und Kongressen – erreichen Sie so direkt und ohne Zeitverzug.

Über das Web-Formular können Sie der Geschäftsstelle ebenfalls Ihre neue Anschrift mitteilen, wenn Sie umziehen.



Datenschutz in der Anwaltskanzlei – Verbot der Bestellung eines Datenschutzbeauftragten?

Stellungnahme des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. zur Bestellung von Datenschutzbeauftragten in Anwaltskanzleien

Von Uwe Meister und Hannes Federrath

In seiner Stellungnahme Nr. 31/2004 vom September 2004 gelangt der Ausschuss Datenschutzrecht der **Bundesrechtsanwaltskammer** im Ergebnis zu der Auffassung, dass

- Rechtsanwälte hinsichtlich der mandatsbezogenen Informationsverarbeitung nicht verpflichtet sind, einen Beauftragten für den Datenschutz zu bestellen,
- die Bestellung eines externen Datenschutzbeauftragten unzulässig ist und
- für die Verarbeitung von Personaldaten der Kanzleien die Bestellung eines Beauftragten für den Datenschutz nach § 4f BDSG eingeschränkt zulässig ist.

Neben einer Reihe von Aufsichtsbehörden (z.B. die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW) und Innenministerien (so z.B. das Innenministerium Baden-Württemberg) hält auch der BvD e.V. diese Rechtsauffassungen in wesentlichen Teilen und im Ergebnis für falsch.

Die Ausführungen der Bundesrechtsanwaltskammer spiegeln ein **fehlerhaftes Verständnis der Umsetzung des Rechts auf informationelle Selbstbestimmung**, wie es seine Ausprägung in einer Vielzahl von Gesetzen und Verordnungen sowohl auf Landes- als auch auf Bundesebene gefunden hat, wider und wirken wenig konstruktiv im Hinblick auf die dringend erforderlichen gemeinsamen politischen Bemühungen aller berufsständischen Institutionen um einen einheitlichen Datenschutz in Deutschland.

1. **Weder das BDSG noch die Vorschriften der BRAO der BORA enthalten** ein gesetzlich normiertes **ausdrückliches Verbot**, in Anwaltskanzleien einen Datenschutzbeauftragten zu bestellen. Auch §§ 4f und 4g BDSG enthalten zu der allgemeinen Verpflichtung, einen Datenschutzbeauftragten zu bestellen, keine Ausnahmeregelung für Anwaltssozitäten oder eine Einschränkung hinsichtlich seiner Aufgaben. Gegen Regelungen bzgl. der Verschwiegenheitsverpflichtung (Berufsgeheimnis) von Berufsständen wird nicht durch die Bestellung eines Datenschutzbeauftragten verstoßen, da dieser typischerweise selbst zur Verschwiegenheit verpflichtet ist (§ 4f Abs. 4 BDSG).

2. Der Umstand, dass berufsspezifische Vorschriften und die darin enthaltenen Berufsgeheimnisse **auch** den Umgang mit Mandanteninformationen regeln, bedeutet nicht, dass hierdurch das **BDSG** als das in Teilen allgemeinere Regelwerk in **toto subsidiär** gegenüber den berufspezifischen Bereichsregelungen ist und damit ausgeschaltet wäre. Ein so verstandenes, möglicherweise berufspolitisch motiviertes Subsidiaritätsverständnis entspricht nicht den allgemein gültigen rechtswissenschaftlichen Regeln zur Lösung von Gesetzeskonkurrenzen (vgl. z.B:

Dieter Schmalz, Methodenlehre für das juristische Studium, 2. Aufl. 1990, Rnd. 67-86).
Auch nach Auffassung des BfD (Ministerialrat Gerhold in einem am 18.10.2004 geführten Gespräch des BfD mit dem Deutschen Steuerberaterverband über das Zugriffsrecht externer Datenschutzbeauftragter auf mandantenbezogene Dateien (http://www.dstv.de/bfdgespraumlch) gehen im Rahmen des die Subsidiaritätsfragen regelnden § 1 Abs. 3 BDSG berufs- und standesrechtliche Vorschriften dem BDSG nur vor, **wenn und soweit** sie **spezifische Datenschutzregelungen** enthalten.

Im Verhältnis des Rechtsanwalts zum Mandanten sind Fragen der Geheimhaltung und etwa Handaktenaufbewahrung in der BRAO bzw. der BORA weitestgehend spezifisch, aber im Hinblick auf beispielsweise technisch-organisatorische Anforderungen des Datenschutzes überhaupt nicht beschrieben. Die BRAO und die BORA können daher (auch) nicht als die die Belange des Datenschutzes abschließend regelnde Rechtsmaterien bezeichnet werden. Zu Abgrenzungsschwierigkeiten zu den übrigen Regelungen des Datenschutzrechts kommt es insoweit nicht, wohl aber sind Regelungslücken durch vorhandene speziellere datenschutzrechtliche Vorschriften zu schließen.

Für die Annahme eines **wertungswidersprüchlichen Eingriffs** in das Strukturprinzip der Regelungen der Berufsgesetze der Anwaltschaft besteht ebenfalls kein Anlass. Soweit der Ausschuss „Datenschutzrecht" der Bundesrechtsanwaltskammer hierbei weitgehend auf das BAG-Urteil vom 11.11.1997 abhebt, welches die Prüfungskompetenz des DSB in Bezug auf die Datenverarbeitung des Betriebsrates betraf und zur teilweisen Unanwendbarkeit des BDSG in jenem Fall führte, **liegt eine vergleichbare Situation** einer dort vom Gericht für notwendig erachteten Neutralität in Bezug auf die Regelungen des Interessenausgleichs zwischen Arbeitgeber und Betriebsrat in den Anwaltskanzleien **nicht vor**. Der dem BAG-Urteil zugrundeliegende Sachverhalt ist nicht auf die Fragen des Datenschutzes in Anwaltskanzleien übertragbar.

Der Datenschutzbeauftragte in Betrieben und der öffentlichen Verwaltung, soweit er dort täglich seine Tätigkeit ausübt, ist als **Gesamtorgan** anzusehen, welches **weder einseitig dem Lager des Arbeitgebers noch dem der Arbeitnehmerschaft zuzuordnen** ist. Er vertritt weder bestimmte berufs- oder standespolitische Interessen, noch Interessen der einen oder anderen Seite eines Mandatsverhältnisses. Er vollzieht vielmehr im weitesten Sinne die Vorstellungen des Gesetzgebers in bezug auf die Erfüllung der Anforderungen des für alle geltenden Datenschutzrechts. Hierbei wird er der jeweiligen individuellen betrieblichen Situation gerecht.
3. Entgegen den Befürchtungen der Bundesrechtsanwaltskammer sind **mandantenbezogene Informationen** gerade nicht Gegenstand datenschutzrechtlicher Überprüfungen. Dies ergibt sich aus dem o.g. Subsidiaritätsprinzip (vgl. z.B. §§ 43 a Abs. 2, 50 BRAO, §§ 2, 19 BORA).

Ein qualifizierter interner oder externer Datenschutzbeauftragter wird in Kenntnis der ihm vor Beginn seiner Tätigkeit vertrauten spezialgesetzlichen Regelungen zum Berufsgeheimnis etc. nicht auf den Gedanken kommen, im Rahmen seiner Tätigkeit entsprechende Zugriffsrechte für sich zu reklamieren. Eine inhaltliche Überprüfung von mandantenbezogenen, verarbeiteten Informationen findet nicht statt, soweit diese Gegenstand einer „Rechtsangelegenheit" sind. Befürchtungen in dieser Hinsicht sind abwegig.

Das in § 4g Abs. 1 Satz 1 BDSG enthaltene Prüfungsrecht betrifft nur die nicht durch spezialgesetzliche Regelungen ausgeschlossenen Bereiche. Solche befassen sich vor allem mit Fragen des technisch-organisatorischen Datenschutzes, z.B.

- sicherer Datenverkehr über Internet, Notebooks, Festplatten, Speichermedien und Telephonie, Fax etc.,
- Zugang zu Datenverarbeitungsanlagen und deren Sicherung,
- Vorkehrungen in Bezug auf Verfügbarkeit von Daten etc.,
- sichere Personaldatenverarbeitung,

– Schutzvorkehrungen gegen Einsichtnahme durch Dritte, Passwörter,
– Vernichtung, Aufbewahrung von Akten nach Sicherheitsstufen nach DIN, soweit geregelt.

Hierzu finden sich in dem die Mandantenbeziehungen regelnden Berufsrecht der Anwälte zumindest derzeit keine Regelungen, die den heutigen Sicherheitsstandards in der Kommunikationstechnik genügen. Insoweit hat die Regelung des § 9 BDSG i.V.m. der Anlage über die Verpflichtung zu technisch und organisatorischen Maßnahmen uneingeschränkte Geltung.

4. Der Ausschuss Datenschutzrecht der Bundesrechtsanwaltskammer **befürchtet Zielkonflikte** zwischen der mandantenbezogenen fachorientierten Anwaltstätigkeit und den Aufgaben eines Datenschutzbeauftragten. Auch in dieser Befürchtung äußert sich mangelndes Verständnis des Datenschutzrechts.

Ein bestellter Datenschutzbeauftragter ist im Rahmen seiner Unterstellung unter einen Auftraggeber oder Dienstherrn in fachlicher Hinsicht stets weisungsfrei (§ 4f Abs. 3 Satz 2 BDSG). Ihm können keine Weisungen erteilt werden, umgekehrt ist er selbst aber auch nicht weisungsbefugt. Er wirkt lediglich auf die Einhaltung von Datenschutzvorschriften hin. Hierunter ist nach gängiger Praxis nichts anderes zu verstehen, als dass er ihm auffällige datenschutzrelevante Sachverhalte erfasst, vermerkt, und - soweit es ihm eingeräumt wird - Änderungsvorschläge unterbreitet.

Ob sich nun ein „Vorgesetzter" an den Empfehlungen eines Datenschutzbeauftragten orientiert oder nicht, obliegt allein diesem selbst, der insoweit verantwortlichen Stelle (§ 3 Abs. 7 BDSG). Der Datenschutzbeauftragte berät und wahrt durch den einer Beratung immanenten Empfehlungscharakter seine Unabhängigkeit, aber auch die des Anwalts.

5. Es ist fraglich, ob Anwaltskanzleien die heutigen Standards sicherer Telekommunikation, z.B. bei der Übermittlung von Daten in das Ausland, einzuhalten in der Lage sind, sofern sie nicht bereits über IT-spezifisches Know-how verfügen. Anwaltskanzleien haben sicher keinen geringeren **Nachholbedarf** als andere Branchen, was die Einführung sicherer Verfahren für den elektronischen Geschäftsverkehr betrifft, z.B. elektronische Signatur nach dem Signaturgesetz, Einsatz von Verschlüsselungstechniken und sicherer E-Mail-Verkehr.

6. Der Berufsstand der Anwälte sollte dafür offen sein, sich mit Hilfe erfahrener Datenschutzbeauftragter den aktuellen Datenschutz- und Datensicherheitsstandards, auch im Interesse der Mandanten, zu nähern.

Ob die Einhaltung dieser Standards durch eigene zum Datenschutzbeauftragten bestellte oder durch externe Datenschutzbeauftragte erfolgt, bleibt letztendlich der Anwaltskanzlei selbst überlassen.

Siehe zu diesem Thema auch:

http://www.datenschutzzentrum.de/wirtschaft/stellungnahme_brak.htm

* * *

Impressum:
Mitgliederzeitung des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. • Geschäftsstelle Gladbeck, Hegemannsweg 32, 45966 Gladbeck, Telefon und Fax (02043) 295602 • Internet: www.bvdnet.de • V.i.s.d.P. Prof. Dr. Hannes Federrath

Bericht aus dem BvD-AK „Externe Datenschutzbeauftragte“

Seit nun gut 2 Jahren besteht unser aktiver Arbeitskreis jetzt schon. Die heutige Ausgabe der BvD-News wollen wir nutzen, um Ihnen, liebe Datenschutzkollegen/Innen, einen Einblick in unsere gemeinsame Arbeit zu geben.

Von Albert Neuner

Derzeit umfasst unser Arbeitskreis 25 Mitglieder, die aus ganz Deutschland viermal im Jahr im Rahmen des Arbeitskreises zusammenkommen. Der damalige Initiator Roland Schäfer vertritt die Interessen unseres AKs nach außen. Derzeit gibt es innerhalb unseres Kreises mehrere Arbeitsgruppen, von denen wir Ihnen, liebe Leser, heute zwei vorstellen möchten.

Unsere erste Arbeitsgruppe arbeitet schon seit Monaten an einer Aufgabenbeschreibung für die Funktion des DSB (intern/extern). Vor kurzem konnten Stefan Staub, Thomas Spaeing, Roland Schäfer und Christian Adolphy innerhalb unseres AKs bereits ein Grundkonzept präsentieren, so dass nach einer ausgiebigen Diskussion die ersten Inhalte detailliert ausgearbeitet werden können. Als Endprodukt soll eine Selbstverpflichtung für externe Datenschutzbeauftragte entstehen, um ein Gütesiegel zu schaffen. So wird es uns als Mitglieder des BvD erstmals möglich sein, uns nach außen hin deutlich für Kunden und interessierte Unternehmen gegenüber den „schwarzen Schafen“ abzugrenzen.

Ebenso ist es unser Ziel, diverse Vorlagen und Formulare für die tägliche Arbeit des DSB zu gestalten. In diesem Zusammenhang arbeiten Monika Egle und Werner Hülsmann derzeit an einer Verschwiegenheitserklärung für das erste Gespräch, mit dem Zweck, Vertrauen zu bilden. Ein Mustervertrag, ein definierter Fragenkatalog und eine FAQ-Liste sollen im Anschluss entstehen. So soll es uns künftig möglich sein, zum einen unsere Vorgehensweise zu erleichtern, indem Synergien genutzt werden. Zum anderen kann so unsere Dienstleistung standardisiert werden, um so transparente, prüffähige Ergebnisse auszuweisen. Diese Unterlagen sollen dann nur Verbandsmitgliedern zur Verfügung stehen.

Wir beschäftigen uns aber auch mit wichtigen Randbereichen unserer Aufgaben. Derzeit arbeitet unser Mitglied Thomas Spaeing an einem Rahmenkonzept für eine Berufshaftpflichtversicherung für Datenschutzbeauftragte. Dieses soll nach einer Angebotsphase mit einem Versicherungspartner abgestimmt werden, um so Verbandsmitgliedern besondere Konditionen zu sichern.

Zusammenfassend möchte ich unsere oberste Zielsetzung unserer gemeinsamen Anstrengungen aufgreifen:

Wir wollen und müssen es erreichen, Qualitätsmaßstäbe innerhalb des BvD zu schaffen und diese im Folgenden dann auf unsere tägliche Arbeit zu transferieren, so dass wir als ein Synonym für Qualität im Bereich Datenschutz auf dem Markt gelten.

So können wir eine Stärkung unseres Berufsverbandes bewirken, denn es soll sich lohnen, ein Mitglied zu sein und daher brauchen wir Alleinstellungsmerkmale und klare Vorteile, die für eine Mitgliedschaft im BvD sprechen.

Stellungnahme zur Video-Überwachung

BvD-AK „Die zukünftige Entwicklung des Datenschutzrechts in Deutschland"

Für nicht öffentliche Räume gibt es derzeit kein Gesetz, das die Videoüberwachung erlaubt. Es ist in diesem Zusammenhang also das allgemeine Persönlichkeitsrecht, zu dem auch das Recht am eigenen Bild gehört, zu beachten.

Eine Berechtigung zum Einsatz einer Videoüberwachung wird allgemein aus dem Hausrecht abgeleitet. Meist werden solche Installationen mit dem Bedarf einer verbesserten Sicherheit begründet.

Dies berechtigt aber weder zu einer versteckten Überwachung noch zu einer uneingeschränkten, flächendeckenden offenen Einsatzmöglichkeit. Aufnahmekameras werden immer kleiner und preisgünstiger und allgemein verfügbar am Markt angeboten. Die freie Verfügbarkeit gewährleistet jedoch nicht, dass deren Einsatz uneingeschränkt rechtmäßig ist.

Aktuelle Gerichtsurteile (z. B. BAG Urteil vom 29.6.2004 1 ABR 21/03) und Medienberichte bis hin zu Darstellungen im Internet zeigen, dass Aufnahmen und Überwachungen praktiziert werden, die unter Verletzung der verfassungsmäßigen Rechte der Betroffenen bis in den besonders geschützten Intimbereich gehen. So sind z. B. im 17. Tätigkeitsbericht der NRW-Beauftragten für Datenschutz und Informationsfreiheit, Bettina Sokol, detaillierte Verstöße dieser Art aufgeführt.

Der § 6b des Bundesdatenschutzgesetzes (BDSG) regelt nur die Verwendung für den öffentlichen Bereich wie folgt:

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
…
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

Damit sind nicht öffentlich zugängliche Bereiche nicht erfasst. Im Vorgriff auf eine erforderliche gesetzliche Regelung zum Videoeinsatz im nicht öffentlichen Bereich empfiehlt der BvD-Arbeitskreis folgende Maßnahmen zur Einhaltung der verfassungsmäßig garantierten Rechte der Betroffenen.

Was sind opto-elektronische Geräte zur Videoüberwachung?

Zur Überwachung werden heute unterschiedlichste Systeme eingesetzt, die geeignet sind, eine optische Überwachung zu ermöglichen. Darunter fallen z.B. Videokameras, Web-Cams, Fotohandys und sonstige Minikameras, die auch versteckt in anderen Geräten

(z.B. in Feuermeldern, Rauchmelder o.ä.) oder Gegenständen eingesetzt werden können.

Voraussetzungen für den Einsatz

Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden. (Grundgesetz für die Bundesrepublik Deutschland Art. 2 Abs. 2, Satz 2)
Eine Überwachung von Personen darf nur dann erfolgen, wenn die Maßnahme geeignet, erforderlich und verhältnismäßig ist. Sie darf nicht verwendet werden, um allgemeine Leistungs- oder Verhaltenskontrollen durchzuführen.
Sie kann demzufolge nur offen und gekennzeichnet sowie mit dem freiwilligen Einverständnis der Betroffenen in Verbindung mit der Zustimmung von Arbeitnehmervertretungen und Datenschutzverantwortlichen erfolgen. Vereinbarungen mit Arbeitnehmervertretungen dürfen nicht die Persönlichkeitsrechte der Betroffenen einschränken. Vereinbarungen, die unter Verletzung der Persönlichkeitsrechte abgeschlossen wurden, sind rechtsunwirksam.
Es ist daher konkret zu prüfen, ob kein anderes, gleich wirksames, aber das Persönlichkeitsrecht weniger einschränkendes Mittel verfügbar ist.
Der Begriff der Verhältnismäßigkeit ist sehr restriktiv auszulegen, wobei insbesondere die Dauer, die Art, die Unausweichlichkeit, die Menge der erfassten Personen und die Datenerhebung und Datenspeicherung sowie die Zahl der zufällig erfassten Personen kritisch zu gewichten sind.
Vor einer Entscheidung zu einer Videoüberwachung sind Zustimmungen durch Datenschutzbeauftragte (Vorabkontrolle gemäß § 4d BDSG) und Arbeitnehmervertretungen (§ 87 Abs. 1 Nr. 6 BetrVG) einzuholen.

Heimliche Überwachungen

Grundsätzlich darf keine verdeckte Überwachung erfolgen. Ist dies in besonderen, begründeten Ausnahmefällen dennoch unverzichtbar, müssen insbesondere folgende Kriterien erfüllt sein
(BAG-Urteil 27.3.2003, 2 AZR 51/02):

- Konkreter, nachgewiesener Verdacht einer strafbaren Handlung oder schwerer arbeitrechtlicher Verfehlungen gegen einzelne Personen, für die eine Wiederholung zu befürchten ist (zur Prävention genügen in der Regel offen installierte Überwachungseinrichtungen),
- weniger einschneidende Möglichkeiten müssen zuvor nachweislich ausgeschöpft sein,
- die Überwachungsmaßnahme darf nur gezielt in einem zeitlich und räumlich eng begrenzten Bereich erfolgen.

Die versteckte Überwachung muss das einzig verbleibende Mittel zur Zweckerfüllung sein.

Was ist im Fall einer zulässigen Installation zu beachten?

Es dürfen keine Personen, Äußerungen oder Verhaltensweisen erfasst werden, die keinen Bezug zum Verwendungszweck haben. Ein Beispiel dafür wäre die Überwachung eines Außenzaunes, die Fußgänger auf dem Bürgersteig erkennbar mit erfasst.
Die Überwachungseinrichtungen sind deutlich sichtbar zu installieren und die Aufnahmebereiche der Überwachungseinrichtungen sind so einzuschränken und auszurichten, dass nur die zur Zweckerfüllung erforderlichen Bereiche erfasst werden.
Aufnahmen von zufällig in den Aufnahmebereich gelangten Personen dürfen nicht verwertet werden und sind nach Möglichkeit umgehend zu löschen. Nicht zur Zweckerfüllung erforderliche, aber im Gerät verfügbare technische Möglichkeiten, z. B. Tonaufzeichnungen, müssen abgeschaltet werden.
Von der Möglichkeit der Aufzeichnung ist nur in Ausnahmefällen Gebrauch zu machen. Der Zugriff auf die Aufzeichnungen ist streng zu beschränken und die Regelung ist vorab schriftlich in Abstimmung mit den Datenschutzbeauftragten und Arbeitnehmervertretungen zu vereinbaren.
Eine empfehlenswerte Regelung dazu ist die Verwendung eines gesplitteten Passworts, das auf mehrere autorisierte Personen verteilt ist. Berechtigte Personen sind der Datenschutzbeauftragte und jeweils ein Mitglied der Arbeitnehmervertretung und des Arbeitgebers.
Die Aufzeichnung hat ausschließlich auf einem separaten System, das für diesen Zweck definiert ist, zu erfolgen. Es ist in einer gesicherten Zone zu positionieren. Zu diesem System dürfen nur schriftlich

autorisierte Personen Zugriff erhalten. Alle Zugriffe, einschließlich der administrativen, sind zu protokollieren, die Protokolle sind durch die Datenschutzbeauftragten auszuwerten.
Die Aufzeichnungen dürfen nicht mit anderen Datenbeständen zusammengeführt werden.
Ein berechtigtes Interesse an der Aufzeichnung von Videodaten bestimmt sich nicht allein nach dem subjektiven Interesse der Betreiber der Anlage, z. B. durch Definition eines Geschäftszwecks, sondern muss objektiv begründbar, Ergebnis einer zuvor vorgenommenen Güterabwägung sein und durch die Rechtsordnung gedeckt sein.
Videoaufzeichnungen, die für den Beobachtungszweck nicht mehr benötigt werden, sind unverzüglich zu löschen. Aufzeichnungen, die für aufklärungsbedürftige Vorkommnisse erfasst wurden, dürfen nur bis zur Erreichung des Beobachtungszwecks gespeichert werden. Aus dieser zweifachen Ausrichtung des Löschungsgebots folgt die Verpflichtung, die Prüfung angefallener Aufzeichnungen zur Bedarfsklärung unverzüglich, d. h. in der Regel innerhalb von ein bis zwei Arbeitstagen, vorzunehmen. (Siehe dazu auch Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 14/4329, 14/4458, Bundestags-Drucksache 14/5793)
Empfehlenswert ist eine automatisierte periodische Löschung, etwa durch Selbstüberschreiben zurückliegender Aufnahmen. Dem Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) kommt in diesem Zusammenhang maßgebliche Bedeutung zu. Er ist einzuhalten. Für die Handhabung von Videoaufzeichnungen sind die Regeln des BDSG anzuwenden.
Eine Datenweitergabe, außer zu Zwecken der Strafverfolgung, ist auszuschließen.
Die Übertragung der Daten von dem Aufnahmegerät zum Speichersystem hat gesichert zu erfolgen, da insbesondere Funk-Verbindungen leicht abgehört werden können.
Permanente Hinweise auf die Überwachungsmaßnahme sind zu installieren. Dazu sind Hinweisschilder in ausreichender Größe (mindestens 180 x 180 mm – DIN-Norm 33450) gut sichtbar und in ausreichender Menge anzubringen.

Die notwendige Klarstellung der Verwendung von Überwachungseinrichtungen soll in der Novellierung zum BDSG eine entsprechende Berücksichtigung finden, wobei primär auch die Regelung für den nicht-öffentlichen Bereich zu ergänzen ist.

Graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen)

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat bei der Verabschiedung der DIN-Norm 33450 (Video-Infozeichen) mitgewirkt.

Im Dezember 2004 wurde vom DIN Deutschen Institut für Normung e.V. die DIN-Norm 33450 (Video-Infozeichen) verabschiedet. Das einheitliche Video-Infozeichen soll dazu beitragen, die Verpflichtung aus dem Gesetz, den Umstand der Videoüberwachung und die verantwortliche Stelle nach § 6b Abs. 2 BDSG durch geeignete Maßnahmen erkennbar zu machen, für alle Anwendungsfälle umzusetzen. *(weiter auf Seite 15)*

• • • • • Technik: Video und Spam • • • • •

Spam-Mail-Behandlung

Arbeitspapier des BvD-AK „Die zukünftige Entwicklung des Datenschutzrechts in Deutschland“

Die Handhabung von Spam-Mails stellt in den Unternehmen der Privatwirtschaft und auch in den Bereichen der öffentlichen Stellen ein zunehmendes Problem dar. Um Denkanstöße zu unterbreiten, wurde zunächst eine Sammlung der Probleme vorgenommen.

1. Beim Ausfiltern von Spam-Mails kann es zu sogenannten „false positives“ (fehlerhaft als Spam Mails interpretierte echte Mails) oder „false negatives“ (nicht erkannte Spam-Mails) kommen.
2. Die Information der adressierten Mitarbeiter über eingegangene Spam-Mails ist auch in Zeiten von Urlaub und Krankheit zu gewährleisten, da false positives erkannt und bearbeitet werden müssen.
3. Die Frage ist zu klären, inwieweit der Arbeitgeber als Spam erkannte Mails direkt löschen darf, oder ob die Mails in einen Quarantäne-Ordner abgelegt werden müssen (siehe Punkt 1)
4. Eine korrekte Datenschutzregelung ist zu treffen, entweder über eine Vereinbarung mit der Arbeitnehmervertretung oder die Zustimmung der Mitarbeiter ist einzuholen.
5. Es ist zu klären, wie technisch gesehen die Filterung praktiziert wird, d.h. inwieweit Einfluss genommen werden kann auf die Erkennungsmechanismen.
6. Durch entsprechende betriebliche Regelungen ist zu gewährleisten, dass es nicht zu Verletzungen des Brief- und Fernmeldegeheimnisses kommt.
7. Die Dauer der Aufbewahrung von in Quarantäneordnern abgelegten Mails ist zu klären.
8. Die Auswirkungen von der Nichtbeachtung/Nichterkennung von false positives ist zu bewerten und durch entsprechende Gegenmaßnahmen sicherzustellen, dass keine rechtsverbindlichen Informationen unbeachtet bleiben.
9. Als sehr gewichtiger Punkt ist eine Festlegung erforderlich die regelt, ob die Privatnutzung von E-Mails, Internet usw. erlaubt, oder generell verboten ist.
10. Das Verbot der Veränderung eingehender Mails gemäß Brief- und Fernmeldegeheimnis (Grundgesetz Art. 10) ist zu beachten bei der Kennzeichnung von als Spam erkannten Mails.
11. Es sind Regelungen zu treffen, die die Handhabung von Protokollen über den E-Mailverkehr, die Auswertung der Protokolle, die Erlaubnis zum Zugriff auf die Protokolldateien und schließlich auch die Löschfristen festlegen.
12. Die Möglichkeit zur Nutzung und die Regeln zur Handhabung von Black- und White-Lists zur Definition erwünschter Spam-Mails (z. B. Newsletter) (Whitelist) oder unerwünschter Mails (Blacklist) ist vorzusehen.

BvD-AK-Empfehlung

Diese nicht abschließende Sammlung von Problemen führte zu folgender BvD-AK-Empfehlung zum Umgang mit Spam-Mails:

1. Alle User einer verantwortlichen Stelle sollten detailliert über die Spam-Mail Problematik informiert werden. Dies sollte die Aufforderung beinhalten, im Internet restriktiv mit der eigenen E-Mail Adresse umzugehen, auf keine Spam-Mails zu antworten. Bei der Beantwortung von Spam-Mail besteht die Gefahr, dass für den Absender von Spam eine Adressbestätigung erzeugt wird, welche dann weiteren

Missbrauch ermöglicht. Aus diesem Grund sollte man ebenso wenig die angebotene Streichung aus dem „Verteiler" beantragen. Die Bedeutung der false positives ist zu erklären und die entsprechende Handhabung darzulegen, die von Seiten der verantwortlichen Stelle geplanten Spam-Abwehraktivitäten sind zu erläutern und in Verbindung damit auch Aussagen über die Privatnutzung zu machen. Nicht zu vergessen ist eine gute Administrierung der eigenen Rechner, um z.B. zu verhindern, dass diese unbemerkt als Spam-Mailserver missbraucht werden. Wird die Privatnutzung verboten, hat der Arbeitgeber uneingeschränkte Zugriffsrechte, was das Filtern von Spam-Mails für ihn weitgehend unproblematisch macht. Wird eine Privatnutzung erlaubt, so sind diverse Zusatzregelungen erforderlich, z. B. ist zu berücksichtigen, dass je nach Art der Filterung das Fernmeldegeheimnis verletzt werden könnte, soweit keine Einwilligung der Nutzer in eine Blockierung bzw. Filterung vorliegt. Eventuell können zusätzliche private E-Mail-Accounts eingerichtet werden. Regelungen zur Erlaubnis für die Mail-Analyse sollten gegebenenfalls im Rahmen einer Betriebsvereinbarung geregelt werden, in der auch Regelungen zum Umfang und der Art einer Privatnutzung getroffen werden können und nach der u. U. eine „Privat"-Kennzeichnung der Mails erfolgt.

2. Eine Vereinbarung mit der Arbeitnehmervertretung ist zu treffen in der z.B. zu regeln ist:
- Privatnutzung von Internet und E-Mail
- Handhabung von Protokollen (ggf. Pseudonymisierung vornehmen)
- Speicher- bzw. Löschfristen
- Einbeziehung des Datenschutzbeauftragten in Vereinbarungen, Aktionen und Auswertungen
- Hinweis darauf, dass die Analyse nicht durch Menschen sondern elektronisch erfolgt und nur eingehende Mails analysiert werden, d.h. interner Mailverkehr ist nicht betroffen.

In Fällen, in denen keine Arbeitnehmervertretung vorhanden ist, sind solche Vereinbarungen direkt mit den Betroffenen Nutzern in schriftlicher Form zu treffen.

3. Die Auswahl eines geeigneten Filterprogramms ist zu treffen unter Berücksichtigung insbesondere der folgenden Punkte:
- Transparenz und technische Aktualität des Filterverfahrens
- hohe Trefferquote (ggf. Referenzen einholen), erforderlich zur Vermeidung von false positives
- Möglichkeit zur Definition von White- und Blacklists
- datenschutzrechtlich unbedenkliche Verfahren (d.h. z. B. mögl. anonymisierte Aufzeichnungen, Verfügbarkeit von Zugriffsregelungen mit Passwortschutz, Quarantäneordner)
- Servicegrad des Softwarelieferanten, Aktualisierungen, Zuverlässigkeit des Laufverhaltens, Konfliktfreiheit zu anderen Softwareprodukten u. ä.

4. Der BvD-AK empfiehlt daher:
- Zur Vermeidung einer Löschung bzw. Blockierung, Ablage der erkannten Spam-Mails in einem Quarantäneordner
- Kurzübersicht an die betroffenen Nutzer, dass Spam-Mails für diese Nutzer im Quarantäneordner liegen, mit der Angabe des Absenders und der Betreffzeile. Die Nutzer mit Kundenkontakten sollten zur regelmäßigen Kontrolle (wegen der false positives) und zum Treffen von Absprachen zur Urlaubsvertretung/Krankheitssituation verpflichtet werden.
- Regelungen zur automatischen bzw. individuellen Löschung der Mails im Quarantäneordner (wenn Punkt Urlaub/Krankheit geregelt ist, ist ein 2-3 Wochenturnus eine gute Lösung.)
- Verfahren für den E-Mailversand zu installieren, die eine Fälschung der Absenderadresse wenn nicht unmöglich, aber doch wesentlich erschweren.

5. Die Nutzer könnten um ein regelmäßiges Feedback an den Administrator gebeten werden zu:
- Anzahl erkannte false positives
- Anzahl eingegangene false negatives
- gewünschte Eintragungen in Black- oder Whitelists

Die Feedbacks sind entsprechend auszuwerten und das Filterprogramm entsprechend anzupassen.

Literatur zum Thema Spam

„Die Rechtslage zum E-Mail-Spamming in Deutschland“, Auswirkungen der BGH-Rechtsprechung und der UWG-Novelle auf die E-Mail-Werbung. Jochen Dieselhorst / Lutz Schreiber in CR 9,/2004 ,S. 680-684

„Virenscanning und Spamfilter - Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co.“, NJW 49/2004, S. 3513-3517, Prof. Dr. Thomas Hoeren

e-f@cts, Ausgabe 17/November 2004 des BMA, Informationen zum E-Business/Schwerpunktausgabe zu Spam (www.bmwa.bund.de) http://www.bmwa.bund.de/Navigation/Technologie-und-Energie/informationsgesellschaft,did=55848.html

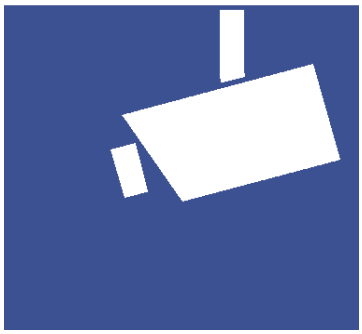
Graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen)

Fortsetzung von Seite 12:

Diese Norm wurde vom Normenausschuss Gebrauchstauglichkeit und Dienstleistungen (NAGD) im DIN erarbeitet. Am Normungsvorhaben beteiligt waren Vertreter der Privatwirtschaft (Schutz- und Wachdienste), von öffentlichen Stellen (Aufsichtsbehörden) und des BvD (Vorstandsmitglied Udo Wenzel). Der Entwurf zur Norm wurde im Mai 2004 veröffentlicht. Im Entwurf wurde nach Meinung des BvD-Vorstands die Pflicht zur Angabe der verantwortlichen Stelle nicht genügend konkretisiert. In seiner Stellungnahme zum Norm-Entwurf hat der BvD deutlichere Formulierungen vorgeschlagen. Der Einspruch des BvDs wurde bei der Verabschiedung der Norm berücksichtigt. Der DIN-Norm 33450 ist eine CD beigefügt. Auf dieser befindet sich das neue Zeichen im pdf-Format, so dass sich schnell und unkompliziert Aufkleber oder Schilder herstellen lassen. Weitere Informationen können der DIN-Pressemitteilung zum Video-Infozeichen entnommen werden. Bestellen kann man die DIN-Norm 33450 beim Beuth-Verlag.

Pressemitteilung des DIN:

http://www2.din.de/sixcms/detail.php?id=18651



„Auch eine Kuh mit der Aufschrift ‚Pferd' bleibt eine Kuh"

Veranstaltungsbesprechung der Tagung DuD 2005 in Berlin

Von Roland Schäfer

Auch in diesem Jahr trafen sich wieder knapp 100 Datenschützer auf der Tagung „DuD 2005" vom 18. bis zum 19. April 2005 in Berlin. Der Name DuD leitet sich von der Fachzeitschrift „Datenschutz und Datensicherheit" ab und setzt deren interdisziplinären Ansatz von Recht und Informatik fort.

Schwerpunktthema war diesmal die Auftragsdatenverarbeitung. Vier Themenreferate waren alleine diesem Schwerpunkt gewidmet. Die Referate und die abschließende Diskussion haben erbracht, dass eine Abgrenzung zwischen der Auftragsdatenverarbeitung nach § 11 BDSG und der im Gesetz nicht genannten Funktionsübertragung schwerer ist, als bislang gedacht. Der Hinweis, Funktionsübertragung sei alles das, was nicht Auftragsdatenverarbeitung ist, half da nicht weiter. Auch die Annahme, außerhalb der Auftragsdatenverarbeitung gebe es ein oder eben kein rechtmäßiges Outsourcing, konnte nicht mehr als ein Annäherungsversuch zu dem Themenkomplex sein. Eine Anwendung der vorgestellten theoretischen Ansätze auf konkrete Fallkonstellationen steht daher noch aus. Zuweilen wurde gestritten, ob kursorische Beispielfälle das eine oder das andere waren, mit den kernigen Worten „Auch eine Frau ist ein Mann im Sinne dieser Vorschrift" oder „Auch eine Kuh mit der Aufschrift ‚Pferd' bleibt eine Kuh".

Weitere Themenreferate folgten. „Haftung und Haftungsvermeidung" zum Datenschutz auf Seiten der Geschäftsführung und des internen oder externen Datenschutzbeauftragten ging leider nur wenig auf die Besonderheiten des Datenschutzes ein. Kann ein weisungsfreier interner Datenschutzbeauftragter auf die vorhandenen Privilegien der Arbeitnehmerhaftung zurückgreifen?

„Abhörmöglichkeiten durch Trojaner und Spyware" war informativ, hat aber inhaltlich nicht viel Neues zu Tage gefördert. „E-Mail Überwachung am Arbeitsplatz in der Schweiz" war eine interessante Ergänzung zu der bekannten deutschen Rechtslage. Die Abgrenzungen nach Schweizer Recht sind dem deutschen Datenschutzrecht im Ergebnis sehr ähnlich, nur der Rahmen der Betriebsverfassung ist in der Schweiz anders gelöst.

„IT Sicherheit in dem SAP-Tool ‚Netweaver'" und das Thema „Security Awareness Kampagnen" sind für sich genommen spannende Elemente der Tagung gewesen. Noch spannender wären die Vorträge gewesen, wenn nicht nur die Sicht der jeweiligen Anbieter der Dienstleistung bzw. des Produktes vorgestellt worden wäre, sondern auch die der Endanwender. Bei dem Thema „Datenschutz in SAP implementieren – Possible Mission" war das genau so. Leider blieb die eine oder andere Rückfrage wegen des Betriebs- oder Geschäftsgeheimnisses des dargestellten Unternehmens unbeantwortet. Hier bedarf es vielleicht eines geschützten Anwenderforums speziell für Datenschützer und SAP-Anwender.

Auch bei dem Thema „RFID – Radio Frequency Identification" sind ein paar Neuigkeiten zu vermelden. Ob allerdings die Umbenennung des Themas in „Ubiquitäre Geschäftsdatenverarbeitung" weiter hilft oder den eigentlichen Problembereich eher vernebelt, mag noch dahinstehen. Dass RFID ein Thema

ist, das im Spannungsverhältnis zur sozialen Verantwortung der Verbraucher steht, scheint zwischenzeitlich auch bei der einschlägigen Industrie angekommen zu sein. Die Fortsetzung der Diskussion um die soziale Verantwortung gegenüber den Arbeitnehmern (Mitarbeiterüberwachung durch RFID-Tags) steht genauso noch an ihrem Anfang, wie die, über deren Verwendung im Verhältnis Bürger-Staat (Reisepass mit RFID oder Geldscheine mit RFID u.s.w). Ob es sich bei dem Gesamtthema nur um ein Akzeptanzproblem handelt oder eines, das normativ durch den Gesetzgeber gelöst werden muss, blieb in der Diskussion strittig.
Insgesamt halten die Diskussionen, die gerade nicht als Podiumsdiskussionen, sondern als Publikumsdiskussionen betitelt sind, das was sie versprechen: Es gibt ausreichend Zeit hierfür, es kommen fundierte Beiträge von der vorhandenen qualifizierten Teilnehmerschaft, gelegentlich werden die Beiträge der Referenten sehr kritisch infrage gestellt, und die Rückfragen sind ganz und gar nicht vorhersehbar.
Der Veranstaltungsrahmen mit den festlichen Mahlzeiten bewegt sich auf einem hohen Niveau. Das Hinweisen auf die Quellen und Besonderheiten der verschiedenen Weinsorten hat dabei sogar schon Kultstatus.
Fazit: Die DuD ist m.E. momentan die beste Tagung, die in Deutschland für Datenschützer angeboten wird.

Datenschutz in Steuerkanzleien

Gemeinschaftsveranstaltung von udis, BvD und privanet e.V.

Von Uwe Meister

In einer Gemeinschaftsveranstaltung von udis, BvD und privatnet am 06.10.2004 in Ulm hatten Steuerkanzleien, Steuerberater und sonstige Interessierte Gelegenheit, sich über die besonderen Anforderungen des Datenschutzes nach dem BDSG mit Blick auf ihren Berufszweig zu informieren. Im Rahmen von Kurzreferaten von Prof. Dr. Kongehl (udis), Rechtsanwalt Glöggler von der Rechtsanwaltskanzlei Gass (Ulm), Vertretern von privanet und der Firma Datev wurde eine allgemeine Einführung in das Datenschutzrecht gegeben, die Qualifikationsvoraussetzungen für bestellte interne oder externe Datenschutzbeauftragte aufgezeigt und mögliche Interessenkollisionen mit externen Dienstleistern z.B. aus der IT-Branche dargestellt. Die sicherheitstechnischen Anforderungen mit Blick auf die besonderen Verhältnisse in Steuerkanzleien wurden herausgearbeitet, vor allem vor dem Hintergrund der dort auftretenden besonderen Datenschutzprobleme.
Im Rahmen der sich anschließenden Diskussion wurde insbesondere seitens des BvD, der durch das Vorstandsmitglied Uwe Meister vertreten war, auf die besondere Bedeutung der beruflichen Qualifikation von externen bestellten Datenschutzbeauftragten hingewiesen, welche wegen der spezifischen datenschutzrechtlichen Verantwortung von Steuerkanzleien nur von erfahrenen und qualifiziert ausgebildeten Datenschutzfachkräften getragen werden könne.
Aufgrund des gezeigten Interesses beabsichtigen die Veranstalter, weitere Veranstaltungen bzw. Vortragsreihen zu diesem Themenkreis durchzuführen.

Neue Nutzungsbedingungen für das Mitgliedschaftslogo

Die Nutzungsbedingungen für das Mitgliedschaftslogo wurden noch einmal vom Vorstand präzisiert.

Nutzungsbedingungen für das Logo "Mitglied im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V."

1. Persönlichen Mitgliedern des BvD ist für die Dauer ihrer persönlichen Mitgliedschaft die Verwendung des BvD-Mitgliedschaftslogos in ihrer Korrespondenz sowie bei Web-Auftritten gestattet.
2. Firmenmitgliedern ist für die Dauer ihrer Firmenmitgliedschaft die Verwendung des BvD-Mitgliedschaftslogos in ihrer geschäftlichen Korrespondenz sowie in ihren Web-Auftritten gestattet.
3. Jede Veränderung sowie eine dem Vereinszweck entgegenstehende Verwendung des BvD-Mitgliedschaftslogos ist unzulässig. Die Verwendung des BvD-Logos ohne den Schriftzug "Mitglied im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V." ist ausdrücklich verboten.
4. Die Erlaubnis zur Nutzung des BvD-Mitgliedschaftslogos kann vom BvD-Vorstand jederzeit widerrufen werden.

Registrierung als externer Datenschutzbeauftragter

Seit Kurzem wird auf der Webseite des BvD den Mitgliedern die Möglichkeit geboten, sich mit Ihrem Profil bei der Geschäftsstelle zu registrieren. Den BvD erreichen immer wieder Anfragen von Firmen, ob externe Datenschutzbeauftragte der jeweiligen Region und mit dem entsprechenden Arbeitsgebiet benannt werden können. Wenn Sie Interesse haben, dass auch Sie benannt werden, dann registrieren Sie sich online unter

http://www.bvdnet.de/