Bezirksregierung Köln

Bezirksregierung, 50606 Köln

An den Präsidenten
des Landtags
Nordrhein-Westfalen
Postfach 10 11 43

40002 Düsseldorf

Zeughausstraße 2-10
50667 Köln
Auskunft erteilt:
Frau Moors

Zimmer:
Durchwahl: (0221) 147 - 2113
Telefax: (0221) 147 - 3185
Aktenzeichen:
(bei Antwort bitte angeben)
21.8-Mo

Datum: 31.01.00

Sehr geehrter Herr Präsident,

für die Einladung zur öffentlichen Anhörung zum Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) bedanke ich mich. Als Anlage ist die Stellungnahme der Bezirksregierung Köln zu der diskutierten Verlagerung der Datenschutzaufsicht von den Bezirksregierungen zur Landesbeauftragten für den Datenschutz Nordrhein-Westfalen beigefügt.

Im Auftrag

(Moors)

Stellungnahme zum Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW);

hier: Diskussion um die Verlagerung der Datenschutzzuständigkeit im nicht-öffentlichen Bereich auf die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

Eine Verlagerung der Datenschutzaufsicht für den nicht-öffentlichen Bereich hin zur Landesbeauftragten für den Datenschutz wird von den Bezirksregierungen Köln und Arnsberg, die die Datenschutzaufsicht in diesem Bereich innehaben, in Übereinstimmung mit dem Innenministerium Nordrhein-Westfalen, Datenschützern anderer Länder sowie der Gesellschaft für Datenschutz und Datensicherung e.V.(GDD) abgelehnt.
Auf die ablehnende Stellungnahme der GDD (GDD-Mitteilungen, Heft 2/99, Seite 4), die überwiegend Datenschützer aus dem Bereich der Privatwirtschaft vertritt, wird verwiesen **(Anlage)**.
Grundlage meiner Ausführungen, die ich für den Regierungspräsidenten Köln abgebe, ist die von Herrn Innenminister Dr. Behrens vorgelegte Stellungnahme der Herren Regierungspräsidenten Köln und Arnsberg.

Ergänzend ist folgendes auszuführen und zusammenzufassen:

1. - Die notwendige Umsetzung der EU-Richtlinie vom 24.Oktober 1995 gebietet in rechtlicher Hinsicht nicht die Verlagerung der Datenschutzaufsicht für den nicht-öffentlichen Bereich auf die Landesbeauftragte für den Datenschutz.
Der Wortlaut der Richtlinie in Artikel 28 Abs. 1, Satz 2 "völlige Unabhängigkeit der Kontrollstellen" eröffnet verschiedene Auslegungsmöglichkeiten, je nachdem, ob die

Formulierung auf die "Unabhängigkeit von den zu Kontrollierenden (Privatwirtschaft)" bezogen wird, oder ob dies als völlige Weisungsunabhängigkeit im ministerialfreien Raum verstanden wird. Die historische Auslegung, die belegt, dass eine Infragestellung des Systems der getrennten Datenschutzkontrolle für den öffentlichen und den nicht-öffentlichen Bereich nicht intendiert war, spricht für die Auslegung, dass die funktionale Unabhängigkeit gemeint ist.

Es wird der Meinung beigepflichtet, wonach verfassungsrechtliche Bedenken gegen die Übertragung des nicht-öffentlichen Aufsichtsbereiches auf die Landesbeauftragte sprechen. Bezug genommen wird auf die Rechtsprechung des Bundesverfassungsgerichts, das vom grundsätzlichen Verbot "ministerialfreier Räume" der Exekutive ausgeht, die der parlamentarischen Verantwortung des Ministers entzogen sind. Es ist hier auch nicht von einer Ausnahme vergleichbar dem ministerialfreien Raum Bundesrechnungshof oder der Datenschutzkontrolle im öffentlichen Bereich auszugehen.

Das Bundesdatenschutzgesetz sieht gravierende Eingriffsbefugnisse gegenüber Unternehmen und Bürgern vor, angefangen vom Betretungsrecht für die Geschäftsräume eines Unternehmens, über die Möglichkeit der Abberufung eines betrieblichen Datenschutzbeauftragten, bis hin zur Möglichkeit zur Untersagung einer technischen Datenverarbeitung. Dies kann bis zur vollständigen Blockierung der Geschäftstätigkeit eines Unternehmens führen.

Nicht ohne Grund wurde auch in der Datenschutzaufsicht im öffentlichen Bereich den Bezirksregierungen die Durchführung von Ordnungswidrigkeitenverfahren mit der je nachdem erforderlichen Verhängung von Bußgeldern

übertragen.
Gegen die verfassungsrechtliche Argumentation kann auch nicht der Einwand des Vorrangs Europäischen Gemeinschaftsrechts durchgreifen, bzw. ein angebliches Verfehlen des Ziels der europäischen Integration. Weder steht und fällt die europäische Einigung mit der Organisation der Datenschutzkontrolle in Deutschland, noch ist nach deutschem Verfassungsverständnis von einem generellen Vorrang des Gemeinschaftsrechts auszugehen.
Zuletzt noch in der Entscheidung des Bundesverfassungsgerichts vom 12.10.1993, 2BvR 2134/92 und 2BvR 2159/92, abgedruckt in der Neuen Juristischen Wochenschrift 1993, Seite 3047 ff., sogenanntes "Maastricht-Urteil", hat das Bundesverfassungsgericht erklärt, dass es seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht in Deutschland in einem "Kooperationsverhältnis zum EuGH ausübe, das Bundesverfassungsgericht sich demnach auf die generelle Gewährleistung der unabdingbaren Grundrechtsstandards beschränken könne". Hierzu zählt das Bundesverfassungsgericht nach der Verlautbarung seiner Pressestelle 39/93 zum Urteil das "unantastbare Demokratieprinzip", um das es hier geht.

2. - Auch die bisherige Aufgabenwahrnehmung durch die Bezirksregierung begründet nicht eine Verlagerung der Aufsicht auf die Landesbeauftragte. Die Bezirksregierung Köln nimmt die Datenschutzaufsicht derzeit mit sieben Mitarbeitern wahr.
Trotz der deutlich geringeren Personalausstattung im Vergleich zur Landesbeauftragten und ständig steigenden Anforderungen qualitativer und quantitativer Art ist sie ihren Aufgaben stets gerecht geworden.
Die Zahl der meldepflichtigen Stellen ist von 300 im

Jahr 1980 auf inzwischen 850 Stellen in 1999 angestiegen. Neben der schwerpunktmäßig ausgeübten Regelaufsicht wurden 1999 etwas über 600 Bürgerbeschwerden bearbeitet.

3. - Die ADV-Ausstattung der Datenschutzaufsicht bei der Bezirksregierung Köln ist sehr gut. Im Bereich der Fortbildung wurden sowohl im technischen als auch im rechtlichen Bereich eigene Initiativen ergriffen und konnten auch in externen Fortbildungsmaßnahmen umgesetzt werden.

4. - Für die Bezirksregierungen ergibt sich aufgrund der Aufgabenstellung im nicht-öffentlichen Bereich eine Konzentration auf bestimmte Themen aus den vorliegenden Verfahren. Dies sind die nach dem Bundesdatenschutzgesetz meldepflichtigen Unternehmen. Schwerpunkte bilden die Bereiche Adressverlage, Auskunfteien, Auftragsdatenverarbeiter (z.B. Servicerechenzentren) sowie Markt- und Meinungsforschungsinstitute. Weiterhin gibt es die sogenannten Anlassaufsichten aufgrund von Beschwerden und Eingaben, die das gesamte Spektrum des Datenschutzes im Bereich der Privatwirtschaft umfassen.
Die Stärke der Bezirksregierungen liegt in der Praxisnähe, die sich in der Kombination unterschiedlicher Anforderungen auch in der Qualifikation und Ausbildung der eingesetzen Prüfer niederschlägt. Im Interesse einer umfassenden Einsetzbarkeit der vorhandenen Prüfer ist Flexibilität gefragt.

5. - Die Beibehaltung der Datenschutzaufsicht bei der Bezirksregierung Köln ist nach hiesiger Auffassung nicht

zuletzt angesichts knapper Mittel kostengünstiger durch die ortsnahe Wahrnehmung der Aufgaben auf der mittleren Verwaltungsebene. Synenergieeffekte gibt es im übrigen auch durch die Ansiedlung des Datenschutzes bei den Bezirksregierungen, durch die Möglichkeit, Wissen aus vielfältigen Fachbereichen (z.B. Medizinalbereich) zu nutzen. Keinesfalls gemeint ist damit die im übrigen bestehende Bündelungsfunktion der Bezirksregierung, die im Datenschutz gerade nicht durch das Zusammenschalten von Informationen erfolgen darf und auch nicht erfolgt.

6. - Gesetzgeberische Defizite wie die bisherige Beschränkung der nicht anlassbezogenen Regelaufsicht nach dem Bundesdatenschutzgesetz auf die meldepflichtigen Unternehmen sowie mangelnde Sanktionsmöglichkeiten bei materiellrechtlichen Datenschutzverstößen sowohl nach dem Bundesdatenschutzgesez als auch nach den "Multimedia"-Gesetzen sind nicht der Struktur der Datenschutzaufsicht bei der Bezirksregierung anzulasten.

7. - Die "neuen" Aufgaben im Bereich "Multimedia"-Datenschutz wurden erfolgreich angegangen.

8. - Der Weg in die Zukunft des Datenschutzes ist nicht die Zentralisierung, sondern die praxisnahe Wahrnehmung der Aufsicht verbunden mit vor allem einer verstärkten Koordination, insbesondere auch im Bereich der länderübergreifenden und aufsichtsbehördenübergreifenden bundesweiten Zusammenarbeit.

Moors

(Moors)

Anlage Az 2614 Bl. 2814

GDD - Mitteilungen

Informationen für GDD-Mitglieder 2/1999

Themen:

Gemeinsames Datenschutz-Colloquium der GDD und der VFH Wiesbaden

„Wege zu einem modernen Datenschutzrecht" war das Leitthema eines von der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) und der Verwaltungsfachhochschule in Wiesbaden am 24. Februar 1999 im Schulungszentrum der Flughafen Frankfurt/Main AG veranstalteten Datenschutz-Colloquiums. Die von Herrn Prof. Peter Gola (Vorstandsmitglied der GDD und Dozent an der Verwaltungsfachhochschule in Wiesbaden) geleitete Veranstaltung zeigte die aktuellen Initiativen zur Novellierung des Bundesdatenschutzgesetzes (BDSG) auf und ging ausgehend vom neuen Hessischen Datenschutzgesetz (HDSG) der Frage nach, inwieweit die Umsetzung der EG-Datenschutzrichtlinie und die Fortentwicklung des deutschen Datenschutzrechts praxisgerecht miteinander verbunden werden können.

Als erstes Bundesland hat Hessen die EG-Datenschutzrichtlinie in das allgemeine Datenschutzrecht umgesetzt. Der Hessische Datenschutzbeauftragte, Prof. Dr. Rainer Hamm, ging anläßlich des Colloquiums insbesondere auf das nach der EG-Richtlinie zu schaffende Datenschutz- und Kontrollkonzept ein. Dabei betonte er die erforderliche völlige Unabhängigkeit der öffentlichen Kontrollstellen. Das Hessische Datenschutzgesetz trage diesem Erfordernis Rechnung, denn es sähe den Landesbeauftragten für den Datenschutz als eine Institution vor, die über keinerlei organisatorische Verbindung zur Exekutive verfüge. Nur wenn der nahezu totale Zugang zu allen Informationen der gesamten hessischen Staatsverwaltung ausschließlich dem Hessischen Datenschutzbeauftragten vorbehalten sei und nicht etwa zusätzlich noch einer Dienst-, Rechts- oder Fachaufsichtsbehörde ermöglicht werde, könne eine hinreichende Abschottung der Daten sichergestellt werden. Die nach Maßgabe der EG-Richtlinie in das Bundesdatenschutzgesetz zu implementierende anlaßfreie Kontrolle mache auch für den nicht-öffentlichen Bereich eine Herauslösung der Kontrollstellen aus dem hierarchischen Gefüge der Exekutivbehörden zugunsten des Anspruchs auf informationelle Selbstbestimmung zwingend erforderlich. Das Hessische Datenschutzgesetz, das die weitestgehende Unabhängigkeit der behördlichen Datenschutzbeauftragten vor Ort und die völlige Unabhängigkeit des Hessischen Datenschutzbeauftragten regele, sei es wert, daraufhin überprüft zu werden, inwieweit es bei der Umsetzung der EG-Richtlinie durch ein neues BDSG als Muster dienen könne.

Der Datenschutzbeauftragte der Fachhochschule Giessen/Friedberg, Hajo Köppen, behandelte die neue Rechtsstellung und neue Aufgaben des internen Datenschutzbeauftragten nach dem neuen Hessischen Datenschutzgesetz. Das neue HDSG setze konsequent die Vorgaben der EG-Datenschutzrichtlinie um und stärke im Interesse des Rechts auf informationelle Selbstbestimmung die Stellung der behördlichen Datenschutzbeauftragten. Die sich hieraus ergebenden neuen Aufgabenstellungen und Kompetenzen bedeuteten für die örtlichen Datenschutzbeauftragten zusätzliche Arbeit und verlangten nach einer vermehrten Unterstützung durch den Hessischen Datenschutzbeauftragten. Nicht

Neue Anschrift:

Herausgeber:
Gesellschaft für Datenschutz und Datensicherung e.V. - GDD
Pariser Str. 37, 53117 Bonn

Telefon: 0228 / 69 43 13
Telefax: 0228 / 69 56 38
Internet: http://www.gdd.de
E-Mail: g-d-d@t-online.de

ausreichend geregelt sei die Verfahrensweise in Konfliktfällen, etwa bei Streit über die Ausstattung oder den Freistellungsumfang des Datenschutzbeauftragten.

Im Rahmen der Diskussion über das neue Hessische Datenschutzgesetz widersprachen insbesondere Vertreter von Datenschutz-Aufsichtsbehörden der von Prof. Dr. Hamm vertretenen Interpretation der „völligen Unabhängigkeit" der Kontrollstellen. Für die Datenschutzaufsicht im nicht-öffentlichen Bereich gelte keine Ausnahme zum grundsätzlichen Verbot ministerialfreier Verwaltung. Die geforderte Unabhängigkeit der Kontrollstellen beziehe sich nur auf die Unabhängigkeit von den zu Kontrollierenden. Das neue HDSG wurde von Teilnehmern des Colloquiums u.a. wegen der Spezialregelungen zum Datenschutz bei Dienst- und Arbeitsverhältnissen gelobt. Andererseits war die mangelnde Verständlichkeit von Gesetzesformulierungen für den Bürger ein Kritikpunkt.

Dr. Thilo Weichert, Stellvertreter des Landesbeauftragten für den Datenschutz Schleswig-Holstein und Vorsitzender der Deutschen Vereinigung für Datenschutz e.V., ging auf die bisherigen Bestrebungen im Zusammenhang mit der Novellierung des BDSG ein und stellte den von ihm miterarbeiteten Entwurf eines Bundesdatenschutzgesetzes von Bündnis 90/Die Grünen als Diskussionsgrundlage bzw. Alternativlösung vor. Dr. Weichert wandte sich gegen Pläne des Bundesinnenministeriums, im Rahmen eines zweistufigen Vorgehens am Referentenentwurf der alten Bundesregierung festhalten zu wollen. Nach Verlautbarungen aus dem Bundesinnenministerium solle in einem ersten Schritt so schnell wie möglich die EG-Datenschutzrichtlinie umgesetzt werden, ergänzt um Regelungen zu Chipkarten, Videoüberwachung, Datenschutz-Audit und Datensparsamkeit. Ein zweiter Schritt solle dann eine umfassende Modernisierung des gesamten Datenschutzrechts bringen. Nach Auffassung von Dr. Weichert sind die EU-Präsidentschaft der Bundesregierung im ersten Halbjahr 1999 und die wegen der nicht fristgerechten Umsetzung drohenden Strafen keine Argumente dafür, sich dem Zeitdruck auf Kosten der Qualität des zu schaffenden Gesetzes zu beugen. Ein Gesetz nach Maßgabe des Entwurfs des Bundesinnenministeriums der alten Regierung sei für den Bürger nicht verstehbar, für Juristen und Informatiker nicht anwendbar. Für Wirtschaft und Verwaltung ergäben sich Rechtsunsicherheit und Anwendungsfehler. Als Grundlage der Novellierung solle - in Ermangelung besserer vorliegender Gesamtalternativen - der Entwurf Bündnis 90/Die Grünen genommen werden. In die Novellierungsdiskussion müßten auch die jüngste Landesgesetzgebung und der umfassende Regelungsvorschlag des Landesbeauftragten für den Datenschutz in Schleswig-Holstein mit einfließen.

v.l.n.r. Herren Prof. Dr. R. Hamm, Dr. T. Weichert, H. Schild, H. Köppen

Herr Dr. U. Dammann

Dr. Ulrich Dammann, Ministerialrat beim Bundesbeauftragten für den Datenschutz, verdeutlichte, daß sich der Termindruck bei der Umsetzung der EG-Datenschutzrichtlinie und die angezeigte Modernisierung des Datenschutzrechts schwerlich miteinander vereinbaren lassen. In diesem Zusammenhang bestätigte er, daß seitens des Innenministeriums über ein Zwei-Phasen-Modell nachgedacht werde. Koalitionsgespräche in Sachen Datenschutz stünden unmittelbar bevor. Im wesentlichen bestehe Konsens über die Einbeziehung von Regelungen zur Zulässigkeit von Videoaufzeichnungen, zum Einsatz von Chipkarten, zum Prinzip der Datenvermeidung und Datensparsamkeit und zumindest teilweise auch zum Datenschutz-Audit. Darüber hinaus gäbe es allerdings auch noch eine Vielzahl von Diskussionspunkten. So denke man im Wirtschaftsministerium beispielsweise darüber nach, die Bestellung eines internen Datenschutzbeauftragten in das Ermessen der Unternehmen zu stellen und wahlweise durch ein staatliches Meldesystem zu ersetzen. Diese Überlegung stieß in der Diskussion angesichts des langjährig bewährten Systems der innerbetrieblichen Selbstkontrolle auf deutliche Ablehnung.

Novellierung des BDSG in 2 Phasen

Die Bundesregierung beabsichtigt, das BDSG in 2 Phasen zu novellieren. In einem ersten Schritt soll möglichst umgehend die EG-Datenschutzrichtlinie umgesetzt werden, ergänzt um Regelungen zu Chipkarten, Videoüberwachung, Datenschutz-Audit und Datensparsamkeit. In einer zweiten Phase soll dann das gesamte

Datenschutzrecht umfassend modernisiert werden.

Ein inoffizielles Arbeitspapier des Bundesministeriums des Innern wurde im Internet veröffentlicht. Dieses kann auch auf der Homepage der GDD (www.gdd.de) unter „Aktuelles" nachgelesen werden.

♦ Datenschutz-Audit

Der Arbeitsentwurf sieht in § 9a die Implementierung eines Datenschutz-Audits für Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen vor. Hiergegen sind erhebliche Bedenken anzumelden.

Bewertung der gesetzlichen Regelung eines Datenschutz-Audits

Bei der Bewertung eines Datenschutz-Audits ist zu differenzieren, ob sich der gesetzliche Anwendungsbereich auf Anbieter von Datenverarbeitungssystemen und -programmen oder generell auf datenverarbeitende Stellen beziehen sollte.

Der Einbeziehung datenverarbeitender Stellen in den Anwendungsbereich eines gesetzlichen Datenschutz-Audits stehen erhebliche Bedenken gegenüber:

- Bisher liegen noch keine Gesetzentwürfe zu Konkretisierung eines Datenschutz-Audits vor. Wissenschaftliche Überlegungen hinsichtlich der Anforderung an die Prüfungen sehen eine Übererfüllung von gesetzlichen Anforderung vor[1]. Bereits die Normung von Qualitätsparametern für ein Datenschutzmanagementsystem, das die gesetzlichen Anforderungen erfüllt, dürfte erhebliche Schwierigkeiten bereiten. Um so schwieriger stellt sich die Festlegung von Normen dar, die eine Übererfüllung verlangen. Die Forderung nach einer Übererfüllung kann zu erheblichen Akzeptanzproblemen der Unternehmen in Datenschutzfragen und zu einer Behinderung der wirtschaftlichen Aktivitäten eines Unternehmens führen.
- Ein Hauptargument gegen ein Datenschutz-Audit bezogen auf das gesamte Datenschutzkonzept einer speichernden Stellen ist die Gefahr, daß das Prinzip der betrieblichen Selbstkontrolle auf dem Gebiet des Datenschutzes unterlaufen wird. Diese hat sich in 22 Jahren seit Verabschiedung der ersten Fassung des BDSG bewährt Das Datenschutz-Audit birgt die Gefahr, daß durch formale Kriterien der Auditierungsinstanzen Unternehmensspezifika keine Berücksichtigung finden. Maßstab der Datenschutzorganisation könnten unflexible Qualitätsmanagementnormen bilden, ohne daß auf Eigenständigkeit und Handlungsspielräume der Unternehmen in Datenschutzfragen Rücksicht genommen würde. Eine starre Orientierung an diesen Normen könnte damit die Unternehmen, die sich einem Audit unterzogen haben, aber in ihrer Organisationsfreiheit im Bereich des Datenschutzes behindern und das dem BDSG zugrunde liegende Angemessenheitsprinzip unterminieren.
- Tragende Säule der betrieblichen Selbstkontrolle auf dem Gebiet des Datenschutzes sind die betrieblichen Datenschutzbeauftragten, die der Geschäftsleitung eines Unternehmens unmittelbar unterstellt und bei der Anwendung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei sind. Eine Ausrichtung der Datenschutzorganisation an Qualitätsmanagementnormen würde die Stellung des betrieblichen Datenschutzbeauftragten schwächen. Bereits jetzt sind Tendenzen erkennbar, daß Geschäftsführungen Datenschutz-Audits in den Unternehmen durchführt, ohne die Datenschutzbeauftragten angemessen zu beteiligen. Dadurch wird die Verantwortung für die Datenschutzorganisation vom Datenschutzbeauftragten als Organ der innerbetrieblichen Selbstkontrolle auf externe Auditierungsstellen übertragen, die von außen den Datenschutz im Unternehmen bestimmen.
- Gegen die gesetzliche Implementierung eines Datenschutz-Audits bezogen auf nichtspezifizierte datenverarbeitende Stellen läßt sich überdies der beachtliche Gesichtspunkt anführen, daß vor allen Dingen für kleine und mittlere Unternehmen, bei denen Datenschutz im Wettbewerbsgeschehen keine besondere Bedeutung zukommt, erhebliche Aufwendungen und Kosten - nicht zuletzt durch die Einhaltung von Qualitätsnormen zur Übererfüllung der gesetzlichen Anforderungen - entstehen können. Dies würde insbesondere in Bereichen, bei denen ein Datenschutz-Gütesiegel, das nach einem erfolgreichen Abschluß eines Auditierungsverfahrens verliehen würde, zu einem Verdrängungswettbewerb dieser kleineren und mittleren Unternehmen führen.
- Die bestehenden Überlegungen zur Einführungen eines Datenschutz-Audits in das BDSG sehen ein freiwilliges Auditierungsverfahren vor. Gleichwohl ist das Argument[2] nicht von der Hand zu weisen, daß aus dieser formalen Freiwilligkeit sehr schnell ein faktischer Zwang entstehen kann. Je nach erbrachten Produkten und Dienstleistungen kann das Datenschutz-Audit nicht unbedingt und unmittelbar zum Geschäftserfolg beitragen.
- Grundsätzlich lassen sich auch Bedenken gegen die Einführung eines Datenschutz-Audits hinsichtlich seiner Aussagefähigkeit anbringen. Ein Audit stellt lediglich eine Momentaufnahme der Datenschutzorganisation im Unternehmen durch externe Auditierer dar. Dem Datenschutz wird jedoch voll umfänglich nur dann Rechnung getragen, wenn dieser als fortwährende Aufgabe und Managementsprozeß begriffen, organisiert und in die Verantwortung des betrieblichen Datenschutzbeauftragten gestellt wird. Eine stichtagsbezogene Momentaufnahme führt nur zu einer Scheinsicherheit in Datenschutzfragen.

Vorgenannte Bedenken gegen ein Datenschutz-Audit lassen sich jedoch relativieren, sofern sich dieses sich auf Anbieter von Datenverarbeitungssystemen und -programmen sowie auf bestimmte DV-Dienstleistungen beschränkt.

- Ein Datenschutz-Audit bezogen auf die Anbieter von Datenverarbeitungssystemen und -programmen trägt positiv zu dem Ziel bei, datenschutzfreundliche Technologien und Produkte auf dem Markt zu fördern. Die Anbieter von Datenverarbeitungstechnologien und -produkten könnten eine Zertifizierung ihrer Produkte

[1] Vgl. Roßnagel, DuD 1997, S. 505 ff.

[2] Vgl. Drews/Kranz, DuD 1998, S.93 f.

bei ihren Marketingüberlegungen positiv zur Geltung bringen.

- Ein Datenschutz-Audit kann auch für bestimmte Dienstleistungen, bei denen die Verarbeitung personenbezogener Daten zum Kerngeschäft gehört, geeignet sein. Anbieter von Multimedia-Dienstleistungen z.B. könnten bezogen auf die Einhaltung der speziellen Datenschutzvorschriften des MDStV bzw. des TDDSG sowie der telekommunikationsrechtlichen Regelungen ein Datenschutz-Gütesiegel als Qualitäts- und Wettbewerbsfaktor im Rahmen ihrer Präsentation und Werbung herausstellen[3].

  Ein Auditierungsverfahren, welches sich auf die Leistungen von Servicerechenzentren beschränkt, kann ebenfalls zur Förderung des Datenschutzes beitragen. Gemäß Art. 17 Abs. 2 EG-Datenschutzrichtlinie hat der für die Verarbeitung Verantwortliche sich von den zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen zu überzeugen. Nach einer Umsetzung dieser Regelung in das BDSG könnte dieses Verfahren erleichtert werden, wenn der Auftragnehmer dem Auftraggeber ein auditiertes Datenschutzmanagementsystem vorlegen kann. Eine Kontrolle vor Ort durch den Auftraggeber ließe sich bei einem auditierten und zertifizierten Dienstleister hinsichtlich des zeitlichen und organisatorischen Aufwandes begrenzen. Es bleibt jedoch auch hier zu berücksichtigen, daß das Audit nur einen zeitabhängigen Ist-Zustand wiedergibt.
- Ein Datenschutz-Audit bezogen auf Anbieter von Multimedia-, Telekommunikations- und DV-Dienstleistungen kann auch eine Minimierung des Kontrollaufwandes für die staatlichen Datenschutz-Aufsichtsbehörden und damit einhergehend für die betroffenen Unternehmen nach sich ziehen. Die nach Umsetzung der EG-Datenschutzrichtlinie anlaßunabhängige Kontrolle kann sich auf das auditierte Datenschutzmanagementsystem beziehen und sich deshalb auf Stichproben beschränken. Dies verringert den Aufwand sowohl für die Aufsichtsbehörden als auch für die betroffenen Unternehmen.

Fazit

Eine gesetzliche Implementierung des Datenschutz-Audits sollte sich nach Auffassung der GDD nicht generell auf datenverarbeitende Stellen beziehen. Die Gefahr eines Unterlaufens der betrieblichen Selbstkontrolle durch eine Fremdkontrolle von externen Auditoren stellt keine dem Datenschutz förderliche Entwicklung dar, da sie die Organisationsfreiheit der Unternehmen auf dem Gebiet des Datenschutzes unterminiert. Weiterhin sprechen das Kosten-Nutzen-Prinzip sowie die Gefahr einer Schwächung der Stellung des betrieblichen Datenschutzbeauftragten gegen einen weiten Anwendungsbereich des Datenschutz-Audits.

Ein Datenschutz-Audit ist jedoch in dem Umfang sinnvoll, wie es das Prinzip der betrieblichen Selbstkontrolle fördert. Anbieter von Datenverarbeitungssystemen, -programmen und DV-Dienstleister könnten ihr zertifiziertes Datenschutzkonzept und ihre technischen Einrichtungen Kunden und Datenschutzverantwortlichen anbieten und zu einem Auswahlkriterium werden lassen. Auch hier jedoch müßten die oben angesprochenen grundsätzlichen Bedenken bei der inhaltlichen Ausgestaltung der Bewertungsmaßstäbe des Audits Berücksichtigung finden.

[3] Vgl. Büllesbach, RDV 1997, S. 237 ff.

♦ Stellung der Aufsichtsbehörde

Eine weitere Besonderheit findet sich eher versteckt in den Regelungen zur Datenschutzaufsicht. Die Vorschrift des § 38 Abs. 1 des BDSG-Entwurfs sieht vor, daß die Datenschutz-Aufsichtsbehörden nur der Rechtsaufsicht der Landesregierung oder der zuständigen obersten Landesbehörde unterstehen. Mit dieser Regelung soll die „völlige Unabhängigkeit" der Datenschutz-Aufsichtsbehörden gem. Art. 28 Abs. 1 EG-Datenschutzrichtlinie umgesetzt werden.

Eine ausschließliche Unterstellung der Datenschutz-Aufsichtsbehörde unter eine Rechtsaufsicht hat erhebliche verwaltungsrechtliche Konsequenzen. Die Datenschutz-Aufsichtsbehörde kann in diesem Fall nicht mehr auf der Ebene der Regierungspräsidenten angesiedelt sein. Diese unterstehen nämlich nicht nur der rechts- sondern auch der weisungsabhängigen Fachaufsicht durch die übergeordnete Landesbehörde. Das Modell einer auf eine Rechtsaufsicht beschränkten Obersten Aufsichtsbehörde entspricht dem Berliner Modell. Dort hat der Berliner Datenschutzbeauftragte die Kontrollkompetenz für den öffentlichen und nicht-öffentlichen Bereich. Eine nur auf Rechtsaufsicht beschränkte Oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich ist der Berliner Senat.

Die Zusammenlegung der Datenschutzkontrolle für den öffentlichen und nicht-öffentlichen Bereich beim Landesbeauftragten führt zu einem bedenklichen Zirkelschuß. Bei der Datenschutzkontrolle im öffentlichen Bereich ist der Landesbeauftragte keiner Kontrolle unterworfen. Bei Kontrolle im nicht-öffentlichen Bereich untersteht er jedoch einer Rechtsaufsicht. In der Folge käme es zu dem unhaltbaren Ergebnis, daß der Landesregierung im Wege der Rechtsaufsicht dem Landesbeauftragten im nicht-öffentlichen Bereich eine bestimmte Auslegung eines unbestimmten Rechtsbegriff des BDSG (z.B. schutzwürdige Belange) vorgeben würde, während der Datenschutzbeauftragte andererseits bei seiner Kontrolle der Landesregierung im öffentlichen Bereich diesen Begriff in seinem Sinne auslegen könnte. Insofern ist den Argumenten beizupflichten, die eine „völlige Unabhängigkeit" der Aufsichtsbehörde nach Maßgabe der EG-Datenschutzrichtlinie so interpretieren, daß diese als Unabhängigkeit von den zu Kontrollierenden zu verstehen ist (vgl. auch Bericht über das Datenschutz-Colloquium).

Modernisierung des Datenschutzes - umfassende Novellierung des BDSG nicht aufschieben

Anläßlich ihrer 57. Konferenz am 25./26. März 1999 haben die Datenschutzbeauftragten des Bundes und der Länder hinsichtlich der Modernisierung bzw. der Novellierung des deutschen Datenschutzrechts die nachfolgend wiedergegebene Entschließung gefaßt:

„Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, daß das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbindung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, daß jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutz-Audit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, daß diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nicht-öffentlichen Bereich muß institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z. B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden."

Notwendig ist nach Auffassung der Konferenz, daß das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies sei eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Gemeinsame Veröffentlichung von Landesbeauftragten

Um den hohen Aufwand bei der parallelen Veröffentlichung der gleichen Texte zu vermindern, haben der Brandenburgische Landesbeauftragte sowie der Berliner Datenschutzbeauftragte beschlossen, künftig bestimmte Texte in einen gemeinsamen Anlagenband aufzunehmen, der gleichzeitig mit dem Tätigkeits- bzw. Jahresbericht erscheint. In ihrem Vorwort zu der in 1998 erschienenen gemeinsamen Veröffentlichung „Dokumente zum Datenschutz 1998" machen die Herausgeber folgende Ausführungen:

„Die Kontrolle des Datenschutzes in Deutschland ist gekennzeichnet durch eine außerordentliche Aufspaltung der Zuständigkeiten: Neben dem Bundesbeauftragte für den Datenschutz, der seine Aufgaben gegenüber Bundesgesetzgeber und -behörden wahrnimmt, gibt es für die Landesverwaltungen die Landesbeauftragten für den Datenschutz sowie für den privaten Bereich die Aufsichtsbehörden für den Datenschutz. Trotz dieser Aufsplitterung ist ein effektiver Datenschutz nur dann gesichert, wenn die beteiligten Gremien ihre Arbeit koordinieren; dies ist auch deswegen erforderlich, weil die geringe Ausstattung der Datenschutzbehörden eine Spezialisierung und eine dadurch mögliche Aufgabenverteilung erzwingen. Seit die ersten Dienststellen des Bundes und einiger Landesdatenschutzbeauftragter Ende der 70er Jahre eingerichtet sind, bietet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder das Forum für die Koordination des Datenschutzes im öffentlichen Bereich. In einer Vielzahl von Beschlüssen und Entschließungen habe sie zur datenschutzgerechten Fortentwicklung der Gesetzgebung, der bürgerfreundlichen Auslegung der bestehenden Gesetze sowie der technisch-organisatorischen Umsetzung des Datenschutzes beigetragen.

Immer mehr Bedeutung gewinnt vor dem Hintergrund der Europäischen Datenschutzrichtlinie und weiterer europarechtlicher Normen mit datenschutzrechtlichem Gehalt auch die Koordination der europäischen Datenschutzbehörden untereinander sowie mit den zuständigen Stellen der Europäischen Kommission. Insbesondere in der aufgrund von Art. 29 der Europäischen Datenschutzrichtlinie gegründete Gruppe werden Dokumente erarbeitet, die für die Arbeit der nationalen Datenschutzstellen von grundlegender Bedeutung sind.

Schließlich gibt es darüber hinaus weltweite Bemühungen, insbesondere auf dem Gebiet der neuen Techniken wie Internet zu einheitlichen Lösungen zu kommen.

Die Ergebnisse all dieser Koordinierungsgremien werden üblicherweise in den Jahresberichten der Datenschutzbeauftragten abgedruckt, so auch in den Tätigkeitsberichten des Brandenburgischen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht sowie des Berliner Datenschutzbeauftragten. ... Die Form der gemeinsamen Veröffentlichung hat u.a. den Vorteil, daß eine fortlaufende, von den Berichten getrennte Dokumentation entsteht.

Die gemeinsame Veröffentlichung soll zudem ein Zeichen dafür sein, daß es auch in den weiterhin getrennten Ländern Brandenburg und Berlin Möglichkeiten der

12/3687

Zusammenarbeit gibt, die die Effizienz beider Seiten steigern können."

Einsicht in das Handelsregister

Schriftstücke, die zum Handelsregister eingereicht sind, können nach § 9 Abs. 2 Satz 1 Handelsgesetzbuch als Abschrift angefordert werden.

Gemäß § 9 Abs. 1 Handelsgesetzbuch darf das Handelsregister selbst von jedermann eingesehen werden, ohne daß die Glaubhaftmachung eines berechtigten Interesses hierfür dargelegt werden muß. Ein berechtigtes Interesse muß daher auch nicht bei der Anforderung von Schriftstücken, die zum Handelsregister eingereicht sind, dargelegt werden. Allerdings müssen die begehrten Schriftstücke so konkret bezeichnet werden, daß dem Registergericht ihr Auffinden in den Registerakten unschwer möglich ist.

Vgl. Entscheidung des Landgerichts Frankfurt vom 12. August 1998 (Az. 3-11 T 52198), auszugsweise veröffentlicht in „Der Betrieb" vom 25. September 1998, Seite 1957.

Bundesregierung: Mehr Sicherheit in der Informationsgesellschaft

Bereits Anfang März hat die Bundesregierung unter der Federführung des Bundesministeriums für Wirtschaft und Technologie (BMWi) eine Initiative für mehr Sicherheit in der Informationsgesellschaft gestartet.

Hauptziel dieser gemeinsam mit dem Bundesinnenministerium aufgelegten Initiative ist es, die Nutzer der weltweiten Informationsnetze zu einem über die tatsächlichen Risiken beim Einsatz der neuen Medien zu informieren, zum anderen aber auch bzgl. eines wirksamen Schutzes zu beraten.

Vor allem soll auch der „normale" Nutzer typische sicherheitsrelevante Fragen beurteilen lernen, ohne ein Informatikstudium absolviert zu haben. Das BMWi merkt dazu an, daß nach einer im September 1998 veröffentlichten Studie lediglich 4% der deutschen Unternehmen ihre elektronische Post verschlüsseln, nur 1% ihre Telefon- und Telefaxkommunikation

Das im Aufbau befindliche Internet-Angebot der Initiative ist abrufbar unter: www.sicherheit-im-internet.de.

Internet-Gefahren für Unternehmen

Vier von fünf deutschen Unternehmen mit Internet-Anschluß sind unzureichend auf die Gefahren vorbereitet, die im globalen Computernetz lauern. Zu diesem Ergebnis kommt eine Studie der Bonner Orbit GmbH, die auf Inter- und Intranet-Projekte spezialisiert ist. Nach Auffassung der Orbit-Experten werde das Thema Datensicherheit häufig nicht ernst genug genommen. Damit sei unbefugten Eindringlingen und Computerviren Tür und Tor in die Rechneranlagen deutscher Firmen geöffnet.

Zwar haben die Unternehmen der Studie zufolge durchweg „Firewalls" errichtet, um unberechtigten Zugriffe auf das Firmennetz vorzubeugen. Allerdings sei nur etwa ein Fünftel der Firmen auf die Gefahren durch neuartige Internet-Technologien vorbereitet. Sechs von zehn der befragten Unternehmen verzichteten ganz auf eine Verschlüsselung der Informationen. Ebenso viele hielten eine zuverlässige Authentifizierung, mit der Benutzer ihre Berechtigung zum Datenzugriff nachweisen müssen, für überflüssig.

Andererseits zeigten sich 75 Prozent der Befragten „sehr besorgt" um die Sicherheit ihrer Computernetze. Mehr als die Hälfte plant in spätestens zwei Jahren zumindestens die wichtigsten Informationen nur noch verschlüsselt ins Unternehmensnetz zu geben.

Neuer Sicherheitstest für Anschluß an das Internet

Erstmals stellt der Datenschutzbeauftragte des Kantons Zürich als unabhängige Behörde den Benutzerinnen und Benutzern des Internets einen Browser-Test zur Verfügung, der es ermöglicht, die Sicherheit des eigenen PC beim Anschluß an das Internet zu überprüfen.

Der Datenschutzbeauftragte des Kantons Zürich hat diese Überprüfungsmöglichkeit für Internet-Benutzerinnen und Benutzer der Verwaltung und für private Personen auf seiner Homepage eingerichtet. Entwickelt wurde der Browser-Test an der Hochschule Rapperswil.

Vielen Surferinnen und Surfern sei nicht bewußt, daß beim Anschluß an das Internet - über feste Leitungen oder über eine Modemverbindung zu ihrem Provider - auf den eigenen PC von Dritten zugegriffen werden könne, wenn Einstellungen unsorgfältig gesetzt würden. In einem solchen Fall könnten bei Rechnern mit den Betriebssystemen Windows 95/98 und NT Dateien gelesen oder sogar Verzeichnisse beschrieben werden. Weiter eröffne sich damit die Möglichkeit der Installation von fremden Programmen auf dem Rechner, die dann Informationen an unbekannte Dritte lieferten. Sensible Daten könnten damit unbemerkt mißbraucht werden.

Um vor solchen Gefahren zu schützen, überprüft der Test, ob die notwendigen Einstellungen korrekt vorgenommen wurden. Damit stellt der Datenschutzbeauftragte des Kantons Zürich erstmals im Internet einen Sicherheitstest zur Verfügung, der dank der Unabhängigkeit des Datenschutzbeauftragten vertrauenswürdig und sicher ist. Von vielen der übrigen Angebote wüßten die Benutzerinnen und Benutzer nicht, was mit den im Test erfaßten Daten wirklich geschehe. Der Datenschutzbeauftragte des Kantons Zürich trägt mit diesem Angebot in Zusammenarbeit mit der Hochschule Rapperswil zur Sensibilisierung in bezug auf Sicherheitsfragen bei und unterstützt die Bemühungen für eine sichere und datenschutzkonforme Benutzung des Internets.

Der Test ist auf der Homepage des Datenschutzbeauftragten des Kantons Zürich verfügbar:
www.datenschutz.ch

Weitere Auskünfte: Dr. Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich, Tel.: 01/259 25 32; Prof. Dr. Peter Heinzmann, Hochschule Rapperswil, Tel.: 055/2224940.