

Rheingasse 8-10  
53113 Bonn

Telefon: 0228/22 24 98  
Telefax: 0228/24 38 470

dvd@datenschutzverein.de  
www.datenschutzverein.de

EU-Registernummer: 64603054524-58

Bonn, 15.01.2011

**Stellungnahme zur Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Gesamtkonzept für den Datenschutz in der europäischen Union“**

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) begrüßt das Vorhaben der Kommission, die Datenschutzrichtlinie 95/46/EG zu modernisieren und an heutige Erfordernisse anzupassen. Sie unterstützt daher alle Bemühungen, das Persönlichkeitsrecht Betroffener auch beim Einsatz neuer Technologien und Anwendungen bestmöglich zu schützen. Die DVD lehnt jedoch alle Ansätze ab, die einseitig zugunsten der Wirtschaft oder aus falsch verstandenem Sicherheitsbedürfnis Bürgerrechte beschneiden und Betroffenen in unangemessener Weise die Kontrolle über die Verwendung ihrer Daten entziehen.

Die DVD merkt insbesondere zu den folgenden aufgeführten Punkten an:

**Zu 2.1.1**

Die DVD teilt die Einschätzung der Kommission, dass die Begriffsdefinition „personenbezogenes Datum“ das Schlüsselkonzept des Datenschutzrechts darstellt.

Um die Geltung des Datenschutzrechts auch für solche Daten sicherzustellen, die erst durch die Verknüpfung mit anderen zu einer Beziehbarkeit führen können, sollte die Begriffsdefinition von missverständlichen Formulierungen befreit werden. Der Zusatz „insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“ wird häufig interessengeleitet fehlinterpretiert und dadurch der Schutz der Grundrechte Betroffener unzulässig verkürzt.

**Zu 2.2.1 und 2.2.4**

Die Kommission plant eine weitere Harmonisierung der Datenschutzbestimmungen auf EU-Ebene und gleichzeitig eine stärkere rechtliche Verankerung der Pflichten der für die Verarbeitung verantwortlichen Stellen. Hierzu will sie unter anderem die Eignung folgender Maßnahmen prüfen:

- A) Verpflichtende Bestellung von unabhängigen, innerbetrieblichen Datenschutzbeauftragten und
- B) Verpflichtende Durchführung einer Datenschutzfolgenabschätzung (im deutschen Recht bisher: „Vorabkontrolle“) in Fällen der Verarbeitung sensibler Daten.

Zu A)

Die DVD steht der europaweiten Einführung innerbetrieblicher Datenschutzbeauftragter aufgrund der Erfahrungen in Deutschland grundsätzlich positiv gegenüber. Sie weist jedoch nachdrücklich darauf hin, dass die Wirksamkeit dieses Modells innerbetrieblicher Selbstkontrolle nur unter bestimmten Rahmenbedingungen funktionieren kann.

Die Unabhängigkeit und Arbeitsfähigkeit des betrieblichen Datenschutzbeauftragten darf nicht nur als Vorschrift auf dem Papier stehen, sondern muss systematisch garantiert werden. Folgende Maßnahmen sind daher unverzichtbar:

- Der Datenschutzbeauftragte darf jederzeit die Datenschutzaufsicht anrufen bzw. sich dort beraten lassen.
- Er hat die Pflicht und das Recht, Beschwerden und Eingaben Betroffener gegenüber dem Arbeitgeber geheimzuhalten.
- Er bekommt ausreichende Arbeitskapazitäten, sowie personelle und finanzielle Unterstützung. Dies schließt auch das Recht auf Teilnahme an Fortbildungsveranstaltungen und Erfahrungsaustausch ein.
- Die Unterstützung muss sich systematisch an der Unternehmensgröße und der Art verarbeiteter personenbezogener Daten orientieren. Es darf nicht hingenommen werden, dass z. B. ein 1000 Personen zählendes Unternehmen eine einzige Person als „Halbtags-Datenschützer“ einsetzt.
- Die Aufgaben des Datenschutzbeauftragten und konkrete Pflichten des Unternehmens ihm gegenüber sind klar zu benennen (Unterweisung der Beschäftigten, geregelte Beteiligung und Beurteilung aller Vorhaben der Datenverarbeitung).
- Der Datenschutzbeauftragte muss Kündigungsschutz genießen.
- Vorhandene Arbeitnehmervertretungen sind bei der Bestellung des Datenschutzbeauftragten zu beteiligen.
- Die Bestellung soll sowohl intern als auch externe möglich sein.

Zu B)

Die DVD sieht die Einführung einer Vorabkontrolle grundsätzlich kritisch, weil dieses Instrument eine zusätzliche Sicherheit für Betroffene vortäuscht, die es nicht einhalten kann.

Sowohl die Richtlinie 95/46/EG als auch die darauf aufbauenden nationalen Datenschutzgesetze legen fest, dass die Verarbeitung personenbezogener Daten nur auf Grundlage bestimmter Zulässigkeitsvoraussetzungen gestattet ist. Es ist daher logisch unabdingbar, dass eine Daten verarbeitende Stelle vor jeder neuen Verarbeitung prüft, ob eine gültige Zulässigkeitsgrundlage besteht – sie die Daten also in der beabsichtigten Art und Weise verarbeiten darf. Es ist daher nicht vorstellbar, dass eine datenverarbeitende Stelle eine neue Verarbeitung oder Anwendung rechtssicher einführen kann, ohne vorher geprüft zu haben, welche rechtlichen Grundlagen sie zu der Verarbeitung berechtigen. Dieser Prozess beinhaltet notwendigerweise auch Erwägungen bzgl. Datensparsamkeit,

Erforderlichkeit notwendiger Schutzmaßnahmen und evtl. Abwägungen des Betroffeneninteresses gegenüber dem berechtigten Eigeninteresse. Das Ergebnis dieses Prozesses muss bei einer ordnungsgemäß organisierten verarbeitenden Stelle, schon allein aus Nachweisgründen, schriftlich dokumentiert werden. Aber auch zur sicheren Umsetzung bedarf es der schriftlichen Form.

Wenn aber schon bei ausnahmslos jeder Verarbeitung personenbezogener Daten die beschriebenen Überlegungen angestellt werden müssen, stellt sich die Frage, welche konkreten Maßnahmen bei einer Vorabkontrolle zusätzlich ergriffen werden sollen, um die Betroffenen bei besonders sensiblen Verarbeitungen zusätzlich zu schützen.

Die Erfahrungen mit der Vorabkontrolle in Deutschland zeigen, dass der Begriff Vorabkontrolle zunehmend zur leeren Hülse verkommt, weil er inhaltlich nicht gefüllt wird, bzw. gefüllt werden kann. Aus dem deutschen Bundesdatenschutzgesetz lässt sich systematisch keine einzige konkrete zusätzliche Schutzmaßnahme für den Fall einer Vorabkontrolle ableiten, die nicht auch bei jedem anderen Verfahren eigentlich ergriffen werden müsste. Textlich wird jedoch der Eindruck erweckt, es müssten zusätzliche Maßnahmen ergriffen werden.

Einige unerwünschte Effekte sind seit Jahren zu beobachten, die den Schutz der Betroffenen im Ergebnis eher herabsetzen: Verarbeitende Stellen verzichten ganz oder teilweise auf die systematische rechtliche Bewertung ihrer Zulässigkeitsgrundlagen bei „normalen“ Anwendungen („das erfordert ja schließlich keine Vorabkontrolle“) und beteiligen den betrieblichen Datenschutzbeauftragten nur unregelmäßig und eher zufällig bei der datenschutzrechtlichen Beurteilung. Sind Vorabkontrollen offensichtlich nötig, so weisen diese, wenn sie denn durchgeführt werden, wegen fehlender Vorgaben sehr unterschiedliche Qualität auf. Dennoch wird den Betroffenen eine ganz besondere Sicherheit vorgegaukelt („wir haben schließlich eine Vorabkontrolle durchgeführt“).

Die DVD hält die Folgenabschätzung in jedem Verarbeitungsfalle für unabdingbar, wenn der Schutz der Betroffenen nach den gesetzlichen Vorgaben garantiert werden soll. Die Festlegung geeigneter Schutzmaßnahmen ist ohne eine solche Abschätzung in keinem Falle möglich. Es wäre daher wünschenswert, verarbeitenden Stellen konkrete Vorgaben für die vor Einführung einer Verarbeitung erforderlichen Abwägungsschritte zu machen. Dies beträfe insbesondere die Pflicht vor Produktivsetzung die Rechtsgrundlage schriftlich festgestellt zu haben, den Datenschutzbeauftragten beteiligt zu haben, die Risiken der Verarbeitung und damit die Schutzbedürftigkeit schriftlich dokumentiert zu haben und die daraus resultierenden erforderlichen Schutzmaßnahmen schriftlich festgelegt zu haben.

Der besonderen Schutzbedürftigkeit bei der Verarbeitung sensibler Daten würde beim derartig organisierten Abwägungsprozess automatisch durch die Ergreifung zusätzlicher Schutzmaßnahmen Rechnung getragen werden müssen. Auf eine missverständliche (und gerne missverstandene) Worthülse wie „Folgenabschätzung“ könnte dann verzichtet werden.

### **Zu 2.3**

Die Kommission möchte die durch den Vertrag von Lissabon geschaffene Rechtsgrundlage nutzen, um Datenschutzfragen bei der polizeilichen und justiziellen Zusammenarbeit erstmals einheitlich zu regeln.

Die DVD begrüßt dies als überfälligen Schritt zur Gewährleistung der europäischen und deutschen Grundrechtsgewährleistungen als Abwehrrechte, vor allem gegen staatliche Eingriffe.

Die Verarbeitung personenbezogener Informationen durch Polizei und Justiz in einer grenzüberschreitenden Zusammenarbeit stellt eine besondere Gefährdung des Rechtes auf informationelle Selbstbestimmung dar, weil die möglichen negativen Auswirkungen von rechtswidrigen oder fehlerhaften Informationen in das Recht auf Leben und körperliche Unversehrtheit, das Recht auf Freizügigkeit und freie Meinungsäußerung sowie auf ein faires Gerichtsverfahren von erheblicher Bedeutung sind.

Die gegenwärtigen Kontrollmechanismen sind intransparent, wenig glaubwürdig und gerichtlicher Schutz für die einzelnen Individuen gegen eine Datenverarbeitung in anderen europäischen Ländern schlicht nicht erreichbar.

Deshalb sieht die DVD in der Einführung eines einheitlichen, kohärenten Rechtsrahmens mit den grundlegenden materiellen und verfahrensrechtlichen Sicherungen und einer öffentlichen, transparenten und völlig unabhängigen Datenschutzkontrollinstanz als notwendige, wenn auch nicht hinreichende Bedingung für einen Abbau des demokratischen Legitimationsdefizits in der europäischen polizeilichen und justiziellen Zusammenarbeit. Dies gilt erst Recht für die europäischen Einrichtungen wie Europol, Eurojust, SIS und ZIS. Auch diese gehören unter die Kontrolle des Europäischen Datenschutzbeauftragten und der Art. 29-Gruppe.

Daneben braucht es spezifische verfahrenssichernde Vorschriften, die in Fällen von legitimen Sicherheitsinteressen eine unbürokratische, kostenfreie und effektive unabhängige europäische richterliche Kontrolle sowie einen vom Parlament gewählten unabhängigen Ombudsmann einführt. So sehen beispielsweise deutsche gesetzliche Vorschriften für Auskunftersuchen gegenüber Geheimdienste in den Fällen, in denen der Geheimdienst sich zum Schutz von Informanten gehalten sieht, eine Auskunft zu verweigern, vor, dass hiervon der jeweilige (parlamentarische) Landesdatenschutzbeauftragte zu informieren ist, der seinerseits die Rechtmäßigkeit und Angemessenheit dieser Entscheidung unabhängig prüfen und im Zweifel seine abweichende Meinung dem Auskunftssuchenden mitteilen kann, der hiergegen eine verwaltungsgerichtliche Entscheidung herbeiführen kann.

## **Zu 2.5**

Die Kommission möchte prüfen, inwieweit die Rechtsstellung und Befugnisse der nationalen Datenschutzbehörden gestärkt, präzisiert und harmonisiert werden können, um den institutionellen Rahmen für eine bessere Durchsetzung der Datenschutzvorschriften zu schaffen.

Die DVD teilt die in der Anhörung geäußerte Kritik und die Befürchtungen nicht, dass der einheitliche Rechtsrahmen durch die europäischen Datenschutzbehörden uneinheitlich umgesetzt und somit die Binnenmarktdimension unterlaufen würde.

Eine institutionelle Stärkung des Art.29-Gremiums durch eine entsprechende personelle und finanzielle Ausstattung durch die Kommission würde hinreichende Grundlagen für die Intensivierung des Meinungs- und Erfahrungsaustausches und damit für eine effektivere Abstimmung in der Umsetzung der aufsichtsrechtlichen Befugnisse schaffen. Ohne Eingriff in die jeweils national gewährleistete Unabhängigkeit kann eine Kohärenz allein durch

gegenseitigen Informations- und Gedankenaustausch bei Beibehaltung des Einstimmigkeitsprinzips in der Art.-29-Gruppe gewährleistet werden.

Die Einführung eines europäischen Datenschutzbeauftragten als einheitliche unabhängige Aufsichtsbehörde für alle öffentlichen und nicht-öffentlichen Stellen in Europa lehnt die DVD wegen des damit verbundenen Verlustes an Effektivität und Unmittelbarkeit entschieden ab.

Zu begrüßen wäre jedoch ein europäisches Zertifizierungsverfahren mit bindendem Charakter für die nationalen Aufsichtsbehörden im Wege eines Konsensverfahrens.

Unklar ist der Vorschlag der Kommission zur „Einführung eines Verfahrens zur Sicherstellung einer einheitlichen Praxis im Binnenmarkt unter der Zuständigkeit der Europäischen Kommission“. Ein solches Verfahren wäre ohne Eingriff in die völlige Unabhängigkeit der nationalen Datenschutzaufsichtsbehörden und der institutionellen europäischen Datenschutzbeauftragten nur denkbar, wenn der neue Rechtsrahmen unmittelbar geltendes europäisches Recht im Wege einer Verordnung vorsieht und die Kommission mit Vollzugs- oder Anordnungsrechten ausstattet. Dann bestünde aber auch keine Veranlassung, erneut sektorspezifische Regelungen („im Binnenmarkt“) einzuführen.

Die DVD lehnt diesen Weg jedoch vor allem unter Hinweis auf den damit einhergehenden Verlust an Flexibilität ab. Die moderne Informations- und Kommunikationstechnik entwickelt sich auch weiterhin in einem so rasanten Tempo, dass die europäische Gesetzgebung hierauf nicht adäquat reagieren kann. Demzufolge müssen die Regelungen in einem Maß abstrakt bleiben, bei dem eine Konkretisierung durch Auslegung der Norm bei neuen Herausforderungen unumgänglich ist. Auch hierfür bietet das Konsensverfahren der unabhängigen Aufsichtsbehörden in der Art.29-Gruppe einen geeigneten institutionellen Rahmen, der bereits als Verfahren zur Sicherstellung einer einheitlichen Praxis ausgestaltet ist. Diese Aufgabe sollte als Zuständigkeit der Art.29-Gruppe in den Rechtsrahmen aufgenommen und damit die gegenwärtige vernünftige Praxis sanktioniert werden.

Die DVD betrachtet mit Sorge die offensichtliche Bereitschaft der Kommission, Sonderinteressen weniger internationaler Unternehmen in anderer Weise gerecht werden zu wollen, als dem Recht jedes Bürgers der Europäischen Union, überall in Europa einheitliche rechtliche Rahmenbedingungen zum Schutz seiner Grundrechte vorzufinden. Wenn es einen nationalstaatsübergreifenden datenschutzrechtlichen Sachverhalt zu bewerten gilt ist das Konsensverfahren der Art.29-Gruppe durchaus ausreichend. Wie das Beispiel der Beratungen zu „google street view“ belegt, waren die nationalen Behörden trotz der Verhandlungstaktik des Unternehmens in der Lage, zu einer einheitlichen datenschutzrechtlichen Bewertung zu gelangen.

Bedenklich inkohärent sind jedoch die Vollzugsmöglichkeiten aufsichtsrechtlicher Anordnungen innerhalb Europas. Hier ist die Kommission aufgefordert den Rechtsrahmen so zu gestalten, dass den Aufsichtsbehörden auch effektive Sanktionsmöglichkeiten zur Verfügung stehen. So sollten die Entscheidungen unmittelbare Rechtswirkung entfalten, umgehend vollzogen werden können und die Sanktionen eine hinreichend abschreckende Wirkung auch für internationale Unternehmen entfalten.

Die DVD begrüßt ausdrücklich die Überlegungen zur Einführung eines Verbandsklagerechtes und der Sammelklagemöglichkeit. Ergänzend könnte ein eigenständiges Klagerecht der jeweiligen unabhängigen Datenschutzaufsichtsbehörde ein

geeignetes Mittel sein, um die Rechte Einzelner auch gegenüber marktmächtigen Unternehmen oder der öffentlichen Verwaltung durchsetzen zu können.

### **Zur Frage des Beschäftigtendatenschutzes**

Die Kommission hat keine Absicht erkennen lassen, den Schutz von Arbeitnehmerinnen und Arbeitnehmern als eigenes Thema in die EU-Richtlinie aufzunehmen.

Die DVD hält es aufgrund des besonderen Abhängigkeitsverhältnisses der Beschäftigten von ihren Arbeitgebern und der Erfahrungen der letzten Jahre in Bezug auf Missbrauchsskandale für unverzichtbar, dass die Richtlinie eigene Schutzvorgaben im Arbeitsverhältnis formuliert. Dies ist erforderlich, weil die Anwendbarkeit von Datenschutznormen im Arbeitsverhältnis mit anderen Schutzziele kollidiert, deren Auflösung nicht den Unternehmen überlassen werden darf. Diese nämlich achten im Zweifel den Datenschutz zu gering und stellen ihr Eigeninteresse automatisch und oft unangemessen über das der Beschäftigten.

Folgende Rahmenvorgaben sollten daher mindestens in die Richtlinie Eingang finden:

- Einwilligungen im Arbeitsverhältnis können nur in Ausnahmefällen als Zulässigkeitsgrundlage dienen. Sie müssen dann bei Erteilung nachweisbar freiwillig und ohne Druck erfolgt sein.
- Datenerhebungen müssen immer beim Beschäftigten erfolgen. Unrechtmäßig erworbene Daten müssen einem Beweisverwertungsverbot unterliegen.
- Das Fragerecht des Arbeitgebers bei der Einstellung muss streng an der Bedeutung und Erforderlichkeit für die angestrebte Beschäftigung orientiert sein.
- Verarbeitet der Arbeitgeber Beschäftigtendaten im Rahmen einer Auftragsdatenverarbeitung durch einen Konzerndienstleister von dem er wirtschaftlich abhängt (z. B. die Konzernmutter), muss dennoch eine wirksame Kontrolle des Auftragnehmers garantiert werden.
- Zum Schutz privater E-Mails müssen klare, dem Schutzniveau des Telekommunikationsgeheimnisses entsprechende Regeln definiert werden, die eine Einsichtnahme und Verwendung durch den Arbeitgeber ausschließen.
- Die Beobachtung und Überwachung von Beschäftigten mittels Video- oder Tonaufnahmen ist grundsätzlich zu untersagen. Der Schutz gilt am Arbeitsplatz und im privaten Umfeld gleichermaßen. Ausnahmen sind nur in streng begrenzten Gefährdungslagen zuzulassen.
- Ärztliche Untersuchungen dürfen nur angeordnet werden, wenn sie gesetzlich vorgeschrieben sind. Die ärztliche Schweigepflicht darf nicht aufgeweicht werden.
- Arbeitnehmervertretungen müssen das Recht erhalten, im Namen von Beschäftigten in Datenschutzfragen zu klagen.