BRUNO SCHIERBAUM

BDSG – die Novellierung 2001

Im Detail wird sich – wenn der jetzt vorliegende Entwurf zum neuen Bundesdatenschutzgesetz (BDSG) beschlossen sein wird – das Eine oder Andere zum Positiven hin verändern; der ›große Wurf‹ aber ist es leider nicht geworden.

Die Bundesregierung hat zum wiederholten Male eine Frist zur Umsetzung einer EG-Richtlinie – im konkreten Fall die zum Datenschutz – verstreichen lassen. Dieser ›Zeitgewinn‹ hat allerdings nicht zu der (dringend notwendigen) grundlegenden Reform des Bundesdatenschutzgesetzes geführt, sondern doch nur zu einer eher bescheidenen Anpassung des deutschen Datenschutzrechts an die Vorgaben der europäischen Datenschutzrichtlinie. Der Spruch: »Was lange währt, wird endlich gut!« ist auf diesen Fall also leider nicht anzuwenden.

Die EG-Datenschutzrichtlinie

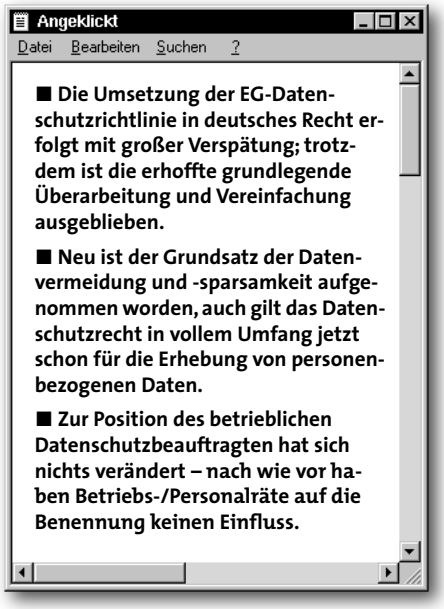
Die Novellierung des Datenschutzrechts wurde erforderlich durch die EG-Datenschutzrichtlinie (EG-DRL) vom 24. 10. 1995, abgeschlossen »zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr«…[1]. Diese Richtlinie hätte spätestens drei Jahre später, also bis bis zum 24. 10. 1998 in deutsches Recht umgesetzt sein müssen, was bis heute nicht geschehen ist.

Die EG-Richtlinie selbst besteht neben einer Begründung und 72 ›Erwägungsgründen‹ aus 34 Artikeln und stellt insgesamt eine kunstvolle ›Collage‹ nationaler Regelungen dar. Der wesentliche Regelungsbereich der Richtlinie wird in Art. 1 EG-DRL so beschrieben, dass die Mitgliedstaaten einerseits bei der Verarbeitung personenbezogener Daten den Schutz der Grundrechte, der Grundfreiheiten und insbesondere der Privatsphäre ›natürlicher Personen‹ gewährleisten, andererseits aber den freien Datenverkehr zwischen den Mitgliedstaaten nicht aus Gründen des Datenschutzes beschränken oder untersagen sollen (mehr zur Richtlinie in: ›EG-Datenschutzrichtlinie – die Frist läuft ab!‹ in cf 10/98 ab Seite 24).

1… RL 95/46 EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; mit den 72 Erwägungsgründen abgedruckt in: Amtsblatt der EG vom 23.11.95 Nr. L 281/31; Dammann/Simitis, EG-Datenschutzrichtlinie – Kommentar 1997; Däubler/Klebe/Wedde, BDSG 1996; Gola/Schomerus, BDSG mit Erläuterungen, 1997.

Die wesentlichen Zielsetzungen der Richtlinie sind somit zum einen der Schutz der Persönlichkeitsrechte – auch Datenschutz genannt – und zum anderen die Gewährleistung des freien Datenverkehrs.

Die EG-DRL strebt dafür eine *Harmonisierung des Datenschutzrechts* an mit der Begründung, dass ein unterschiedliches Datenschutzniveau in den einzelnen Mitgliedstaaten die Übermittlung von Daten von einem Mitgliedstaat in einen anderen verhindern kann. So ist zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten unerlässlich.



Da den Mitgliedstaaten zugleich die Fähigkeit abgesprochen wird, die erheblichen Unterschiede ihrer nationalen Rechtsvorschriften selbst abzubauen, »ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich« *(so die Begründung in Erwägungsgrund 9 der EG-Datenschutzrichtlinie)* – nämlich der Erlass der EG-Datenschutzrichlinie.

Stand der Novellierung des BDSG

Wie gesagt: Die Umsetzung hierzulande hat auf sich warten lassen, nunmehr aber liegt ein Novellierungsvorschlag mit einer entsprechenden Begründung vor. Am 14. Juni 2000 hat das Bundeskabinett den Gesetzentwurf zur Novellierung des Bundesdatenschutzgesetzes beschlossen und der Bundesrat hat in seiner Sitzung vom 29. 9. 2000 die Modernisierung des Datenschutzrechtes grundsätzlich befürwortet. In den Änderungsvorschlägen, die der Bundesrat gleichwohl beschlossen hat, wird unter anderem die Streichung der Regelung zum ›Datenschutzaudit‹ (audit = Prüfung) gefordert. Jetzt läuft das übliche parlamentarische Verfahren, mit dem Inkrafttreten des Gesetzes wird für Anfang 2001 gerechnet.

Übrigens: Wegen dieser deutlich verspäteten Umsetzung der EG-Datenschutzrichtlinie hat die EU-Kommission im Januar 2000 die Einleitung der dritten Stufe des ›Vertragsverletzungsverfahrens wegen Nicht-Umsetzung der EG-Datenschutzrichtlinie‹ gegen Deutschland bekannt gegeben. Das ist der formelle Beschluss der Kommission, die Bundesrepublik Deutschland zu verklagen. Und bei dieser Klage wird es nicht nur um die schleppende Novellierung des Bundesdatenschutzgesetzes gehen, sondern auch um die Umsetzung der Richtlinie in den einzelnen Bundesländern, die in der Mehrzahl ebenfalls noch nicht abgeschlossen ist (siehe dazu: ›Datenschutzgesetz – Hessen vorn‹ in cf 8-9/99 ab Seite 17 und ›Ein großer Schritt voran!‹ in cf 4/00 ab Seite 29).

Wie auch immer: Die Umsetzung der EG-DRL soll hierzulande nun in einem zweistufigen Verfahren realisiert werden. Im ersten Schritt soll das BDSG an die Vorgaben der EG-Datenschutzrichtlinie angepasst und im zweiten Schritt das gesamte Datenschutzrecht mit dem Ziel einer umfassenden Modernisierung auf den Prüfstand gestellt werden. »Modernisierung bedeutet in diesem Zusammenhang Vereinfachung und Verschlankung des Datenschutzrechts, denn nur wenn die Bürgerinnen und Bürger die ihnen zustehenden Rechte

kennen und verstehen, können diese auch eingefordert werden« – so die Ausage der Bundestagsabgeordneten Tauss (SPD) und Özdemir (Bündnis 90/Die Grünen) in der Zeitschrift ›Recht der Datenverarbeitung‹, Heft 4/00, Seite 144. Was ›Verschlankung‹ bedeutet oder bedeuten könnte, lässt sich daran abschätzen, dass allein für den Bereich des Bundes über 100 Gesetze bereichsspezifische Datenschutzbestimmungen enthalten!

Zudem soll im Zusammenhang mit der Modernisierung des Datenschutzes ein ›Arbeitnehmerdatenschutzgesetz‹ und ein ›Informationszugangsgesetz‹ auf den Weg gebracht werden.

Die Änderungen des BDSG

Im jetzt vorliegenden Entwurf des neuen Bundesdatenschutzgesetzes (BDSG-E) wird die nach der EG-Richtlinie zwingend erforderliche Anpassung des bestehenden BDSG vorgenommen, wobei der Entwurf an dem vertrauten – aber keineswegs übersichtlichen – Aufbau des BDSG weitgehend festhält. Weiterhin wird im BDSG-E *entgegen* der Vorgabe der EG-Richtlinie die Trennung zwischen öffentlichem und nicht-öffentlichem Bereich beibehalten, so dass auch das neue BDSG nur für den nicht-öffentlichen Bereich (also für alle Privatbetriebe) und für den öffentlichen Bereich des *Bundes* gelten wird; für die öffentlichen Stellen *der Länder* hingegen werden nach wie vor die jeweiligen – und zum großen Teil noch zu novellierenden – Landesdatenschutzgesetze gelten.

Die notwendig gewordenen Änderungen sind dabei – wie schon angedeutet – in die bestehende Struktur des BDSG und vor allem in den ersten Abschnitt (›Allgemeine und gemeinsame Bestimmungen‹) nur eingeschoben worden, so dass nun im BDSG-E beispielweise der § 4 um die §§ 4 a bis 4 g anwächst. Und da die Regelungen zum betrieblichen Datenschutzbeauftragten in den §§ 4 f und 4 g BDSG-E verankert sind, können folgerichtig dann die §§ 36 und 37 BDSG entfallen.

Der Anwendungsbereich des BDSG-E

Weil – wie schon erwähnt – das BDSG-E entgegen der EG-Datenschutzrichtlinie nach wie vor die Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich kennt, gelten der erste, vierte und fünfte Abschnitt des BDSG-E wie bisher auch für den öffentlichen *und* den nicht-öffentlichen Bereich, der

zweite Abschnitt gilt *allein für den öffentlichen Bereich des Bundes* und der dritte Abschnitt *allein für den nicht-öffentlichen Bereich*.

Der sachliche Anwendungsbereich des BDSG-E erstreckt sich auf die *automatisierte* (also computergestützte) Verarbeitung personenbezogener Daten.

> *§ 3 Abs. 2 Satz 1 BDSG-E:*
> *Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.*

Da der bisher geltende ›Dateibezug‹ (das aktuelle BDSG gilt nur bei Verarbeitung und Nutzung personenbezogener Daten ›in oder aus Dateien‹) im novellierten BDSG entfallen soll, werden künftig auch Bild- und Tonträger dem BDSG unterliegen.

Der ›Dateibezug‹ bleibt lediglich bei der *nicht-automatisierten* Verarbeitung von Bedeutung:

> *§ 3 Abs. 2 Satz 2 BDSG-E:*
> *Eine nicht-automatisierte Datei ist jede nicht-automatisierte Sammlung personenbezogener Daten, die gleichtartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.*

Diese neue Definition einer ›nicht-automatisierten Datei‹ wird dazu führen, dass künftig auch die in vielen Betrieben noch verwendeten, nach Alphabet oder sonst einem System geordneten Karteikästen mit beispielsweise Adressensammlungen vom BDSG erfasst werden. Akten und Aktensammlungen hingegen, die nicht ›gleichartig aufgebaut‹ und auch nicht ›nach bestimmten Merkmalen‹ zugänglich sind, fallen auch künftig nicht unter den Anwendungsbereich des BDSG.

Ausgenommen vom BDSG-Anwendungsbereich ist zudem eine Erhebung, Verarbeitung und Nutzung von Daten, soweit sie ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – das noch geltende BDSG enthält eine ähnliche Regelung.

Die in § 1 Abs. 3 BDSG enthaltenen Ausnahmen für automatisierte Dateien, die aus ausschießlich ›verarbeitungstechnischen Gründen‹ *vorübergehend* erstellt werden, entfallen mit der Novellierung – auch hier wird der Anwendungsbereich also ausgeweitet.

Anwendung von ausländischem Datenschutzrecht

Mit der Novellierung des BDSG kann es in der Bundesrepublik künftig auch in Einzelfällen zur Anwendung von ausländischem Datenschutzrecht kommen. Nach § 1 Abs. 5 BDSG-E wird das Bundesdatenschutzgesetz *keine Anwendung* finden, sofern eine in einem *anderen EU-Mitgliedstaat* gelegene ›verantwortliche Stelle‹ (im noch geltenden BDSG ›speichernde Stelle‹ genannt) personenbezogene Daten *im Inland,* also hier in der Bundesrepublik erhebt, verarbeitet oder nutzt. Vielmehr ist in solchen Fällen auch in der Bundesrepublik das Datenschutzrecht des entsprechenden Mitgliedstaates anzuwenden.

Erfolgt die Erhebung, Verarbeitung und Nutzung allerdings durch *eine Niederlassung* der EU-ansässigen ›verantwortlichen Stelle‹ (die in der Regel ein Unternehmen sein dürfte), dann ist das BDSG anzuwenden. Die Begründung für diese etwas verwirrende Regelung verweist auf den Begriff ›Niederlassung‹, wie er in § 42 Abs. 2 Gewerbeordnung definiert ist. Demzufolge ist eine Niederlassung immer dann vorhanden, wenn der Gewerbetreibende einen *zum dauernden Gebrauch eingerichteten, ständig oder in regelmäßiger Weise von ihm benutzten Raum für den Betrieb seines Gewerbes* besitzt. Dies bedeutet, dass die Schwelle zur Annahme einer Niederlassung (und damit für die Gültigkeit des BDSG) zwar nicht besonders hoch ist, dass Zurechnungsprobleme in der Praxis aber dennoch nicht auszuschließen sind.

Die Regelung verliert noch dadurch weiter an Brisanz, dass in § 1 Abs. 5 BDSG-E klargestellt wird, dass die Zuständigkeit der (deutschen) Aufsichtsbehörden unberührt bleibt, auch wenn im Einzelfall EU-ausländisches Datenschutzrecht zur Anwendung kommt.

In jedem Fall findet das BDSG Anwendung, wenn eine außerhalb der EU gelegene verantwortliche Stelle personenbezogene Daten in der Bundesrepublik Deutschland erhebt, verarbeitet oder nutzt.

Besondere Arten personenbezogener Daten

Neu aufgenommen sind in § 3 Abs. 9 BDSG-E besondere Arten personenbezogener Daten, die in der Literatur als ›sensitive‹ (empfindliche) Daten bezeichnet werden: »Besondere Arten personenbezogener Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.« Eine solche besondere ›Sensitivität‹ gibt oder gab es nach deutschen Datenschutzverständnis bisher nicht. Ausschlaggebend ist vielmehr der Zusammenhang, in dem ein personenbezogenes Datum steht oder genutzt wird.

So können vermeintlich harmlose Daten in Verbindung mit anderen Daten durchaus eine besondere ›Sprengkraft‹ erlangen. Nach dem BDSG-E unterliegen die erwähnten sensitiven Daten jedoch einem besonderen Schutz. Soll zum Beispiel die Verarbeitung dieser sensitiven Daten durch eine Einwilligung der betroffenen Person abgesichert werden, dann muss sich die Einwilligung ausdrücklich (und nicht etwa pauschal) auf diese Daten beziehen. Zudem muss vor der Erhebung, Verarbeitung oder Nutzung von sensitiven Daten eine Vorabkontrolle – das heißt: eine datenschutzrechtliche Technikfolgenabschätzung – durchgeführt werden (§ 4 d Abs. 5 und 6 BDSG-E).

Datenvermeidung und Datensparsamkeit

Nach § 3 a BDSG-E haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen prinzipiell an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Damit wird der Grundsatz der Datenvermeidung und -sparsamkeit erstmalig in das BDSG aufgenommen. Eine vergleichbare Regelung findet sich in § 3 Abs. 4 des Teledienstedatenschutzgeset-

zes. Wie dort soll auf diese Art die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten bereits durch eine entsprechende Gestaltung der Systemstrukturen soweit wie möglich vermieden werden. Anders ausgedrückt: Es soll zu einem verstärkten Einsatz datenschutzfreundlicher Techniken kommen, um so Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen von vornherein gar nicht erst aufkommen zu lassen.

So dürften beispielsweise Kantinenabrechnungssysteme, die zu zahlende Beträge direkt vom Lohn oder Gehalt abziehen, *nicht* der Vorgabe der Datenvermeidung und Datensparsamkeit entsprechen. Anders wäre dies bei einem Kantinenabrechnungssystem, bei dem der Beschäftigte eine Magnet- oder Chipkarte an einem Automaten mit einem Geldbetrag auflädt, um dann damit zu bezahlen. In diesem Fall werden keine personenbezogenen Daten des Beschäftigten verarbeitet, der Grundsatz der Datenvermeidung und Datensparsamkeit ist also eingehalten.

Ebenfalls neu beinhaltet der § 3 a Satz 2 BDSG-E den Vorrang anonymer und ›pseudonymer‹ Formen der Datenverarbeitung. Sie sollen der ›verantwortlichen Stelle‹ erleichtern, aus ihrer Sicht erforderliche Datenverarbeitungen durchzuführen und zugleich dem Grundsatz der Datenvermeidung/Datensparsamkeit Rechnung zu tragen. Der Begriff des Pseudonymisierens wird neu in das BDSG eingeführt:

§ 3 Abs. 6a BDSG-E
Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

Unverändert geht das novellierte BDSG von einem ›Verarbeitungsverbot mit Erlaubnisvorbehalt‹ aus – das heißt: Eine Datenerhebung, -verarbeitung und -nutzung ist nur zulässig, soweit ...

... das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder
... der Betroffene eingewilligt hat.

Bisher allerdings gelten für die *Erhebung* personenbezogener Daten durch nicht-öffentliche Stellen geringere Anforderungen als für die Verarbeitung und Nutzung – nach § 28 Abs. 1 BDSG genügt hier ein Handeln ›nach Treu und Glauben‹. Nach § 4 Abs. 1 BDSG-E wird jetzt aber auch schon das Erheben von Daten den gleichen Zulässigkeitsvoraussetzungen unterworfen wie deren Verarbeitung und Nutzung.

Dieses Einbeziehen der Erhebung wird unter Anderem zur Folge haben müssen, dass alle in den Unternehmen eingesetzten Personalfragebogen nach der Novellierung des BDSG zu überprüfen sind!

Zusätzlich wird in § 4 Abs. 2 BDSG-E festgelegt, dass die Erhebung von Daten *beim Betroffenen selbst* zu erfolgen hat. Es wird also das Prinzip der *Direkt-Erhebung* verankert, das bisher (laut § 13 Abs. 2 BDSG) nur für den öffentlichen Bereich des Bundes galt. Dieser Grundsatz, dass personenbezogene Daten immer beim Betroffenen direkt zu erheben sind, ist unmittelbarer Ausfluss des Volkszählungsurteils und des dort formulierten ›informationellen Selbstbestimmungsrechts‹: Der Betroffene soll wissen, wer wann welche Daten über ihn sammelt, speichert und verarbeitet.

Der Gesetzesentwurf sieht jedoch Ausnahmen vor, wenn ...

... eine Rechtsvorschrift die Erhebung vorsieht oder zwingend voraussetzt oder
... die Verwaltungsaufgabe oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder wenn
... die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde.

Diese Ausnahmen kommen aber nur dann zum Tragen, wenn es *keine* Anhaltspunkte dafür gibt, dass das ja immer zu berücksichtigende ›Schutzinteresse des Betroffenen‹ nicht vielleicht schwerer wiegen könnte als das Interesse eines Unternehmens oder einer Behörde an einer Datenerhebung.

Dadurch, dass jetzt auch die ›Erhebung‹ von Daten in die Frage der Zulässigkeit einbezogen ist, müssen unter anderem alle Personalfragebogen auf den Prüfstand!

In § 4 Abs. 3 BDSG-E ist eine Unterrichtung des Betroffenen im Falle der Direkterhebung verankert und zwar in Bezug auf:

- die Identität der verantwortlichen Stelle;
- die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung;
- die Kategorien von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung rechnen müsste.

Eine der Rechtsgrundlagen für eine zulässige Datenerhebung, -verarbeitung oder -nutzung kann bekanntlich das BDSG selbst sein. Basis dafür ist auch im BDSG-E der § 28. Eine der wesentlichen Änderungen besteht auch hier in der Einbeziehung der Erhebungsphase. Das heißt: Schon eine Erhebung personenbezogener Daten darf nur in einer sehr engen Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses erfolgen, wobei gleichzeitig eine Interessensabwägung zwischen dem berechtigtem Interesse der verantwortlichen Stelle und dem schutzwürdigen Interesse des Betroffenen zu erfolgen hat.

Zusätzlich sind bereits bei der Erhebung die Zwecke konkret festzulegen,

für die die Daten verarbeitet oder genutzt werden sollen.

Einwilligung als rechtliche Basis

Die Einwilligung als eine mögliche Basis für die rechtmäßige Datenerhebung, -verarbeitung oder -nutzung ist in einem gesonderten Paragrafen geregelt. Die im aktuellen BDSG verankerten Vorgaben – so etwa die Schriftform – wurden beibehalten. Für die ›sensitiven‹ Daten schreibt § 4 a Abs. 3 BDSG-E – wie schon gesagt – vor, dass sich eine entsprechende Einwilligung ›ausdrücklich‹ auf diese Daten beziehen muss:

§ 4 a Abs. 1 BDSG-E
Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

§ 4 a Abs. 3 BDSG-E
Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

Übermittlung personenbezogener Daten ins Ausland

Zu den für die Praxis bedeutsamen Neuerungen gehören auch die Vorgaben zum grenzüberschreitenden Datenverkehr (siehe: ›Grenzüberschreitender Datentransfer‹ in cf 8-9/99 ab Seite 36).

Bisher gibt es für den nicht-öffentlichen Bereich im BDSG keine eigenständige Regelung für die Übermittlung von Daten ins Ausland. Die EG-Richtlinie dagegen enthält eine differenzierte Regelung, die auch für den öffentlichen Bereich gilt, wobei die EG-DRL innerhalb der Mitgliedstaaten der Europäischen Union den ›freien Datenverkehr‹ vorsieht. Vor diesem Hintergrund nun stellt § 4 b Abs. 1 BDSG-E den innergemeinschaftlichen Datentransfer dem inländischen gleich. So ist ein Datentransfer von München nach Paris künftig genau so zu behandeln wie ein Datentransfer von München nach Hamburg. Für die Übermittlung der Daten gelten die in § 4 BDSG-E enthaltenen Zulässigkeitsvoraussetzungen (siehe oben).

Die Datenübermittlung in ein Drittland *außerhalb der Europäischen Union*, ist im Grundsatz nur dann zulässig, wenn das Drittland ein *angemessenes Datenschutzniveau* gewährleistet. Ob ein ›angemessenes Datenschutzniveau‹ besteht, kann die übermittelnde Stelle anhand der in § 4 b Abs. 3 BDSG-E enthaltenen Vorgaben eigenständig prüfen. So wird die Angemessenheit des Datenschutzniveaus unter Berücksichtigung aller Umstände beurteilt werden müssen, die bei einer Datenübermittlung von Bedeutung sind. Dieses können insbesondere die Art der Daten, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für die betreffenden Empfänger geltenden Rechtsnormen sowie die für den Empfänger geltenden Standesregeln und Sicherheitsmaßnahmen sein. Dabei trägt gemäß § 4 b Abs. 5 BDSG-E die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung.

Die zur Feststellung der Angemessenheit erforderlichen Ermittlungen zum Datenschutzrecht sowie zu sonstigen im Empfängerland geltenden Rechtsnormen bis hin zu Standesregeln können sehr aufwändig sein. Deshalb sieht Artikel 25 Abs. 6 EG-DRL vor, dass die EU-Kommission für ein Drittland allgemein die Feststellung in Bezug auf ein angemessenes Datenschutzniveau treffen kann. Gleiches gilt für den Fall, dass ein angemessenes Datenschutzniveau *nicht* besteht. Positive Feststellungen wurden zwischenzeitlich für Ungarn und die Schweiz getroffen.

Für den Datenverkehr mit den USA gibt es eine besondere Regelung. Da in den USA weder eine umfassende Datenschutzgesetzgebung besteht noch eine solche beabsichtigt ist, wäre ein allgemeines Feststellen eines ›angemessenen Datenschutzniveaus‹ wenig aussichtsreich gewesen. Gerade wegen der engen wirtschaftlichen Beziehungen zwischen den Mitgliedstaaten der EU und den USA ist ein Rechtsrahmen mit der Bezeichnung ›US International Safe Harbor Principles‹ oder kurz ›Safe Harbor‹ (= sicherer Hafen) für die Daten aus Europa vereinbart worden. US-Unternehmen können sich (freiwillig) den Regeln des ›Safe Harbor‹ unterwerfen und werden dadurch priviligierte Emfpänger personenbezogener Daten aus Europa.

Für europäische Unternehmen bedeutet dieses in Bezug auf die Prüfung eines ›angemessenen Datenschutzniveaus‹ eine erhebliche Erleichterung. Sie brauchen sich lediglich durch Einsicht in die derzeit in Vorbereitung befindliche Liste des US-Handelministeriums davon zu überzeugen, dass ihr Geschäftspartner dem ›Safe Harbor‹ angehört.

Auch für den Fall, dass ein Empfängerland kein angemessenes Datenschutzniveau gewährleistet, lässt § 4 c BDSG-E jedoch Ausnahmen zu, wie beispielsweise die Einwilligung durch den Betroffenen. Aber: Soll durch eine Einwilligungserklärung der Transfer von Beschäftigtendaten rechtmäßig gestaltet werden, so stellen diese Einwilligungserklärungen immer ›Personalfragebogen‹ dar, unterliegen also der Mitbestimmung. Darüber hinaus besteht im Einzelfall die Möglichkeit den Datentransfer in ein Drittland ohne angemessenes Datenschutzniveau durch die Aufsichtsbehörde genehmigen zu lassen und zwar dann wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts vorweist. Diese Garantien können sich u.a. aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben.

Meldepflicht neu geregelt ...

Automatisierte Verarbeitungen sind von nicht-öffentlichen Stellen (also Unternehmen) vor ihrer Inbetriebnahme der Aufsichtsbehörde (z.B. dem Landesbeauftragten für den Datenschutz) zu melden. Für öffentliche Stellen gilt eine

entsprechende Meldepflicht gegenüber dem Bundesbeauftragten für den Datenschutz. Die deutsche Delegation hat nun in Brüssel mit Erfolg darauf hingewiesen, dass aus deutscher Sicht im Bereich der Privatwirtschaft ein zur staatlichen Aufsicht mindestens gleichwertiger Datenschutz auch durch eine ›qualifizierte Eigenkontrolle‹ gewährleistet werden kann – das heißt konkret: durch die Bestellung eines betrieblichen Datenschutzbeauftragten. Deshalb entfällt die Meldepflicht sowohl nach EG-DRL wie auch BDSG-E, »wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat« (§ 4 d Abs. 2 BDSG-E). Für Kleinbetriebe, bei denen nicht mehr als vier Arbeitnehmer personenbezogene Daten erheben, verarbeiten oder nutzen, entfällt sowohl die Meldepflicht wie auch die Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu bestellen. In diesem Bereich käme eine Meldepflicht also in erster Linie bei ›Datenverarbeitung im Auftrag‹ zum Tragen.

Der Inhalt der Meldepflicht wird in § 4 e BDSG-E festgelegt. Im Rahmen der Meldepflicht sind demnach folgende Angaben zu machen:

- Name oder Firma der verantwortlichen Stelle;
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen;
- Anschrift der verantwortlichen Stelle;
- Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung;
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien;
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;
- Regelfristen für die Löschung von Daten;
- eine geplante Datenübermittlung in Drittstaaten;
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Datenschutz und Datensicherungsmaßnahmen gemäß § 9 BDSG angemessen sind.

Bei besonderen Risiken: Vorabkontrolle

Über die ohnehin vorgegebene Zulässigkeitsprüfung (§ 4 in Verbindung mit § 28 BDSG) hinaus ist bei Datenverarbeitung *mit besonderen Risiken für den Betroffenen* eine ›Vorabkontrolle‹ durchzuführen. Soweit *automatisierte* Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen mit sich bringen, hat diese Prüfung vor Beginn der Verarbeitung zu erfolgen. Um welche Verarbeitungen es sich dabei handeln könnte, wird vom Gesetz nur recht abstrakt umschrieben. Eine Vorabkontrolle ist aber in jedem Fall dann durchzuführen, wenn ...

... besondere Arten personenbezogener Daten – die so genannten sensitiven Daten – verarbeitet werden oder

... die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Dieses bedeutet, dass in Bezug auf den Arbeitnehmerdatenschutz eine Vorabkontrolle beispielsweise bei Telekommunikationsanlagen, Personalabrechnungs- und Informations-Systemen, bei Betriebsdaten-Erfassungs-Systemen sowie bei Produktionsplanungs- und -steuerungs-Systemen durchzuführen sein wird, da die Verarbeitung personenbezogener Daten mit Hilfe dieser Systeme immer zur Leistungs- oder Verhaltenskontrolle führen kann.

Aber auch hier sieht das BDSG-E wieder Ausnahmen vor: In beiden etwas konkreter aufgeführten Fällen ist die Vorabkontrolle nur dann durchzuführen, wenn der Verarbeitung weder eine gesetzliche Verpflichtung noch eine Einwilligung zu Grunde liegt und sie auch nicht im Rahmen eines Vertragsverhältnisses erfolgt.

Zuständig für die Vorabkontrolle ist gemäß § 4 d BDSG-E der Beauftragte für den Datenschutz, der sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden hat.

Bei Datenverarbeitung ›mit besonderen Risiken‹ (z. B. Verarbeitung ›sensitiver‹ Daten, wie ethnische Herkunft, Partei- und Gewerkschaftszugehörigkeit) ist eine Vorabkontrolle durchzuführen.

Beauftragter für den Datenschutz

Die Vorschriften über den Datenschutzbeauftragten und seine Aufgaben wurden im BDSG-E in den allgemeinen Teil des Gesetzes (Abschnitt 1) übernommen. Für den öffentlichen Bereich des Bundes stellt dies eine Neuerung dar, da es bisher für diesen Bereich keine gesetzlichen Vorschriften gab. Die Bestellung eines Datenschutzbeauftragten wäre somit sowohl für den öffentlichen Bereich als auch den nicht-öffentlichen Bereich verpflichtend. Nur Kleinbetriebe sind von der Bestellung eines betrieblichen Datenschutzbeauftragten freigestellt (siehe oben).

Eine solche Ausnahme ist nach der EG-Datenschutzrichtlinie zwar nicht vorgesehen, der bundesdeutschen Gesetzgeber hält sie aber weiterhin – eher willkürlich – aufrecht. Dies ist schon deshalb problematisch, weil die Gefährdung der Persönlichkeitsrechte ja nicht allein von der Zahl der Beschäftigten abhängt. Im Gegenteil kann davon ausgegangen werden, dass eine Person an einem entsprechend ausgestatteten PC erheblich mehr ›anstellen‹ kann als etwa eine Bedienungsmannschaft von zwanzig Beschäftigten in einem Rechenzentrum der siebziger Jahre (also zu der Zeit in

der die Ausnahmeregelung entstanden ist).

In Bezug auf die Person des betrieblichen Datenschutzbeauftragten, deren persönliche Voraussetzungen, das verankerte Beanachteiligungsverbot und auch die zu erfüllenden Aufgaben hat sich gegenüber den Vorgaben der §§ 36 bis 37 BDSG nichts Grundlegendes verändert. Der Gesetzgeber versäumt es hier vor allem, ein Beteiligungsrecht der Arbeitnehmervertretung bei der Bestellung des betrieblichen Datenschutzbeauftragten gesetzlich zu regeln oder auch einen besonderen Kündigungsschutz zu verankern. Es ist nicht nachzuvollziehen, warum gerade in diesen Punkten eine Gleichstellung mit den Beauftragten im Bereich des Umweltrechts (wie z. B. Immissionsschutzbeauftragter, Störfallbeauftragter, Abfallbeauftragter) nicht verankert wird.

Mit der Novellierung kommen auf den betrieblichen Datenschutzbeauftragten zwei neue Aufgaben zu:

- Der betriebliche Datenschutzbeauftragte muss gemäß § 4 d Abs. 5 BDSG-E die Vorabkontrolle durchführen.
- Der betriebliche Datenschutzbeauftragte hat in den Fällen, in denen keine Meldepflicht besteht, auf Antrag jedermann die gemäß § 4 g Abs. 2 BDSG-E zu führenden Übersichten verfügbar zu machen. Damit soll die Transparenz in Bezug auf die Verarbeitung personenbezogener Daten erhöht werden.

Zusätzlich ist künftig gesetzlich geregelt, dass sich die Betroffenen (z. B. die Arbeitnehmer) an den betrieblichen Datenschutzbeauftragten wenden können (§ 4 f Abs. 5 BDSG-E).

Eine weitere Neuerung besteht darin, dass nicht-öffentliche Stellen, die eine Vorabkontrolle durchführen müssen oder die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung erheben, verarbeiten oder nutzen (z. B. Adresshändler, Auskunfteien), unabhängig von der Anzahl der Arbeitnehmer einen betrieblichen Datenschutzbeauftragten bestellen müssen (siehe § 4 f Abs. 1 BDSG-E).

Automatisierte Einzelentscheidungen

Der § 6 a BDSG-E stellt die Umsetzung des Artikels 15 der EG-DRL dar und ist insoweit eine Besonderheit, als nicht die *Zulässigkeit* der Datenverarbeitung selbst geregelt wird, sondern es werden Entscheidungsabläufe reguliert: Nach § 6 a Abs. 1 BDSG-E dürfen nämlich Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen (z. B. eine Kündigung), nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, wenn diese der Bewertung einzelner Persönlichkeitsmerkmale dienen.

Der Grundgedanke dieser Vorschrift ist dem französischen Recht entnommen und beruht auf dem Grundgedanken, dass Entscheidungen, die die Bewertung einer Person beinhalten und daher das Persönlichkeitsrecht zentral berühren, nicht einem Computerprogramm überlassen werden dürfen.

Aber wie so oft, gibt es auch hier Ausnahmen, die in § 6 a Abs. 2 BDSG-E niedergelegt sind. Das Verbot gilt also nicht, wenn ...

... die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und einem Begehren des Betroffenen *stattgegeben* wurde oder wenn ...

... die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer automatisierten Entscheidung mitgeteilt wird.

In § 6 a Abs. 3 BDSG-E schließlich ist für den Fall automatisierter Entscheidungen ein besonderes Auskunftsrecht verankert, das sich auch auf die Logik des Verarbeitungsvorgangs selbst bezieht. Die Probleme für die praktische Umsetzung dieser Vorgabe sind jedoch nicht zu übersehen, da heutige Software äußerst umfangreich und komplex aufgebaut ist. In jedem Fall muss der logische Aufbau der automatisierten Entscheidungsfindung, so wie er sich im Programmablauf vollzieht, der betroffenen Person verständlich gemacht werden. Sie muss verstehen können, in welcher Weise aus ihren konkreten personenbezogenen Daten bestimmte Bewertungen oder Klassifizierungen abgeleitet werden und welche Bedeutung diesen Werten im Verarbeitungssystem zukommt.

Video-Überwachung

In § 6 b BDSG-E wird erstmals eine Rechtsgrundlage zur Video-Überwachung geschaffen. So ist die *Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen* nur zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke zulässig. Und auch das nur, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen könnten. Diese Vorschrift erfasst allerdings nur öffentlich zugängliche Räume wie etwa Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhalten.

In der Gesetzesbegründung heißt es dazu, dass für nicht öffentlich zugängliche Räume – also in Privatbetrieben – besondere Regelungen, beispielsweise im Rahmen eines Arbeitnehmerdatenschutzgesetzes, erforderlich sind. Dies könnte in der Praxis zu erheblichen Irritationen führen, denn aus der Gesetzesbegründung könnte man durchaus den Schluss ziehen, dass Betriebe mit Video-Überwachung diese bis zu einer gesetzlichen Regelung einstellen müssten. Praktisch aber wird man wird wohl davon ausgehen müssen, dass die Zulässigkeit einer Video-Überwachung in nicht öffentlich zugänglichen Räumen den Vorgaben des § 4 in Verbindung mit § 28 BDSG (Zulässigkeit der Datenverarbeitung) und *zusätzlich* gemäß § 4 d Abs. 5 BDSG-E der *Vorabkontrolle* unterliegt.

Bei Video-Überwachung in öffentlich zugänglichen Räumen dient die Regelung in § 6 b Abs. 2 BDSG-E erhöhter Transparenz. Denn die Regelung besagt, dass durch geeignete Maßnahmen so-

wohl der Umstand der Beobachtung wie auch die verantwortliche Stelle erkennbar zu machen ist. Geeignete Maßnahmen könnten deutlich sichtbare Hinweisschilder sein.

Schadensersatz

In § 7 BDSG-E wird die Reglung des Artikels 23 EG-DRL umgesetzt und damit im Bundesdatenschutzgesetz erstmals eine eigenständige Anspruchsgrundlage für die Haftung geschaffen, die sowohl für den öffentlichen wie den nicht-öffentlichen Bereich gilt. Fügt eine ›verantwortliche Stelle‹ dem Betroffenen durch eine nach dem BDSG oder nach anderen Vorschriften über den Datenschutz *unzulässige* oder *unrichtige* Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten schuldhaft einen Schaden zu, ist diese dem Betrofenen zum Schadensersatz verpflichtet. Die Ersatzpflicht soll nach § 7 Abs. 1 BDSG-E entfallen, soweit die ›verantwortliche Stelle‹ die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Anlage zu § 9 BDSG

Die in § 9 BDSG vorgegebenen Datenschutz- und Datensicherungsmaßnahmen bleiben auch im neuen BDSG bestehen. Die Anlage zu § 9 BDSG wird jedoch von vormals zehn auf acht Zielvorgaben gekürzt (siehe info-Kasten rechts)

Datenschutzaudit

Die Regelung zum Datenschutzaudit (audit = Prüfung, Kontrolle) entspricht dem § 17 Mediendienste-Staatsvertrag der Länder. Nach § 9 a BDSG-E können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige Gutachter prüfen und bewerten lassen. Das Ergebnis der Prüfung können diese Stellen veröffentlichen. Die näheren Anforderung an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter sollen gemäß § 9 a BDSG-E durch ein Gesetz geregelt werden.

info

Anlage zu § 9 BDSG-E

Die acht neuen Gebote des Datenschutzes

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden zu verwehren.

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

4. Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

5. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgelegt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

6. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

7. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8. Getrennte Verarbeitung

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Widerspruchsrecht

In § 35 Abs. 5 BDSG-E werden die Benachrichtungs- und Auskunftsrechte um ein *Widerspruchsrecht* ergänzt. Das Widerspruchrecht greift ein, soweit der Betroffene der Datenverarbeitung bei der verantwortliche Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Das Widerspruchsrecht gilt nicht, wenn eine Rechtsvorschrift zur Erhebung Verarbeitung oder Nutzung von personenbezogenen Daten verpflichtet. Ob dieses Widerspruchsrecht allerdings im Arbeitsleben überhaupt zum Tragen kommt, ist sehr fraglich.

Aufsichtsbehörde

Die wichtigste Veränderung für die Praxis ist der Wegfall der so genannten Anlasskontrolle. Nach dem aktuellen BDSG kann die Aufsichtsbehörde nur dann tätig werden, wenn ihr hinreichende Anhaltspunkte dafür vorliegen, dass eine nicht-öffentliche Stelle gegen Datenschutz-Vorschriften verstoßen hat oder wenn ein Betroffener einen konkreten Verstoß begründet darlegt.

Nach der Novellierung des Bundesda-

tenschutzgesetzes kann die Aufsichtsbehörde *jederzeit* tätig werden.

Datenschutz durch Mitbestimmung

Betriebs-/Dienstvereinbarungen stellen ein wichtiges Regelungsinstrument für die Zulässigkeit der Verarbeitung von Beschäftigtendaten dar. Entsprechende Regelungen werden insbesondere in Ausübung des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG (bzw. § 75 Abs. 3 Nr. 17 BPersVG) getroffen. Diese Regelungen gehen auch weiterhin als ›andere Rechtsvorschriften‹ im Sinne des § 4 Abs. 1 BDSG dem Datenschutzgesetz vor, verdrängen also in ihrem Regelungsbereich das BDSG (siehe dazu: ›Vereinbarung contra Selbstbestimmung?‹ in cf 1/01 ab Seite 24).

In keinem Fall jedoch dürfen Betriebs-/Dienstvereinbarungen schlechtere Regelungen enthalten als das BDSG. Natürlich verändern sich mit der Novellierung des BDSG auch Art und Umfang des Überwachungsrechts nach § 80 Abs. 1 Nr. 1 BetrVG (§ 68 Abs. 1 Nr. 2 BPersVG). Zudem wird bei der Umsetzung der Mitbestimmung bei Personalfragebogen nach § 94 BetrVG (§ 75 Abs. 3 Nr. 8 BPersVG) die Einbeziehung der Erhebung in § 4 BDSG und die damit verbundenen engere Zulässigkeit der Erhebung von Daten zu berücksichtigen sein. Und nicht zuletzt müssen Betriebs-/Personalräte an Schulungen zur neuen Rechtslage teilnehmen können.

Bruno Schierbaum, BTQ Niedersachsen, Oldenburg, Telefon 0 44 11 / 8 20 68; eMail: **schierbaum@btq.de**