Das neue Bundesdatenschutzgesetz – Novellierung mit erheblicher Verzögerung

Das Bundesdatenschutzgesetz (BDSG) ist mit erheblicher Verzögerung novelliert worden. Das Gesetz ist einen Tag nach der Verkündung im Bundesgesetzblatt[1] am 23. Mai 2001 in Kraft getreten und ist mit diesem Tag von allen öffentlichen Stellen des Bundes und allen so genannten „nicht-öffentlichen" Stellen (Privatbetriebe, Vereine etc.) umzusetzten. Übergangsfristen sind nur für bereits laufende Anwendungen in § 45 BDSG vorgesehen. Es ist festgelegt worden, dass Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die mit dem In-Kraft-Treten des BDSG bereits begonnen haben, binnen drei Jahren mit den Vorschriften dieses Gesetzes in Einklang zu bringen.

Die Novellierung des Datenschutzrechts ist erforderlich geworden durch die EG-Datenschutzrichtlinie (DRL) vom 24. 10. 1995 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"[2]. Die EG-Datenschutzrichtlinie hätte bereits bis zum 24. 10. 1998 in deutsches Recht umgesetzt werden müssen. In diesem Artikel sollen die wichtigsten Neuerungen des BDSG dargestellt werden.

Die EG-Datenschutzrichtlinie als Anlass der Novellierung

Die DRL selbst besteht aus 34 Artikeln, einer Begründung zur Richtlinie, den 72 Erwägungsgründen und stellt insgesamt eine „kunstvolle Collage"[3] nationaler Regelungen dar. Der wesentliche Regelungsbereich der Richtlinie wird in Art. 1 DRL dahingehend umschrieben, dass die Mitgliedstaaten sowohl den **Schutz der Grundrechte und Grundfreiheiten** und insbesondere der Privatsphäre natürlicher Personen bei der **Verarbeitung personenbezogener Daten** gewährleisten, als auch den **freien Datenverkehr** zwischen den Mitgliedstaaten nicht aufgrund des Datenschutzes beschränken oder untersagen[4]. 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 DRL verfolgt den Zweck der Harmonisierung des Datenschutzrechts mit der Begründung, dass das unterschiedliche Datenschutzniveau in den einzelnen Mitgliedstaaten die Übermittlung von Daten von einem Mitgliedstaat in einen anderen verhindern kann[5]. 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[6]. Da den Mitgliedstaaten die Fähigkeit abgesprochen wird, die erheblichen Unterschiede ihrer nationalen Rechtsvorschriften selbst abzubauen[7], „ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich"[8]. In den der Umsetzung dienenden Vorschriften selbst oder durch Hinweis bei der amtlichen Veröffentlichung müssen die Mitgliedstaaten Bezug auf die Richtlinie nehmen. Durch dieses Zitiergebot werden die Mitgliedstaaten veranlasst, sich selbst, der Öffentlichkeit und der Kommission Rechenschaft abzulegen, auf welche Weise die Umsetzung gewährleistet wird[9].

Das neue BDSG

Nunmehr liegt das BDSG als Artikel 1 des „Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze" vor[10].

Mit der erfolgten Novellierung des BDSG ist nur ein erster Schritt der Modernisierung des Datenschutzrechts erfolgt. In einem zweiten Schritt soll das ge-

1) Vgl. Bundesgesetzblatt, Jg. 2001 Teil I Nr. 23, S. 904 ff.

2) 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; abgedruckt mit den 72 Erwägungsgründen 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; vgl. hierzu: Schierbaum, EG-Datenschutzrichtlinie – die Frist läuft ab! Computer Fachwissen 1998, S. 24 ff.

3) Vgl. Dammann/Simitis, (Fn. 2), Einleitung, Anm. 13.

4) Zur Richtlinie vgl. ausführlich: Dammann/Simitis; (Fn. 2); Schierbaum, EG-Datenschutzrichtlinie – Änderungsbedarf des BDSG und Auswirkungen auf die Beteiligungsrechte von Betriebsräten, ArbuR 1998, S. 350 ff.; Schierbaum, Nichtumsetzung der EG-Datenschutzrichtlinie, PersR 1998, S. 502 ff.; Brühann/Zerdick, Umsetzung der EG-Datenschutzrichtlinie, CR 7/96, S. 436 ff; Wohlgemuth, Auswirkungen der EG-Datenschutzrichtlinie auf den Arbeitnehmerdatenschutz, BB 13/96, S. 693 ff.

5) Vgl. Erwägungsgrund 7 zur EG-Datenschutzrichtlinie.

6) Vgl. Erwägungsgrund 8 zur EG-Datenschutzrichtlinie.

7) So gab es bis in die 90er Jahre keine Datenschutzgesetze in Belgien, Spanien und Griechenland; vgl. hierzu: Kopp, Der EG-Richtlinienvorschlag zum Datenschutz in Europa, DuD 1993, S. 11.

8) Erwägungsgrund 9 zur EG-Daetnschutzrichtlinie.

9) Vgl. Dammann/Simitis (Fn. 2), Art. 32 Anm. 3.

10) Das Artikelgesetz enthält nicht nur in Artikel 1 das geänderte BDSG, sondern die Änderung weitere Gesetze wie Änderung des Bundesverfassungsschutzgesetzes (Art. 2); Änderung des MAD-Gesetzes (Art. 3), Änderung des BND-Gesetzes (Art. 4), Änderung des Sicherheitsüberprüfungsgesetzes (Art. 5), Änderung des Bundesgrenzschutzgesetzes (Art. 6), Änderung des Bundeskriminalamtgesetzes (Art. 7), Änderung des Sozialgesetzbuches (Art. 8), Änderungen des Finanzverwaltungsgesetzes, des Postgesetzes, des Soldatengesetzes, des Wehrpflichtgesetzes, der Strafprozessordnung, des Strafvollzuggesetzes, des Zollverwaltungsgesetzes, des Bundesdatenschutzgesetzes (Art. 8a–8 h) und In-Kraft-Treten (Art. 9).

samte 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."[11] Was „Verschlankung" bedeutet, kann daran abgeschätzt werden, dass zum einen das aktuell novellierte BDSG unübersichtlicher und komplizierter geworden ist als das alte BDSG und zum andern, dass allein für den Bereich des Bundes über 100 Gesetze bereichsspezifische Datenschutzbestimmungen enthalten. In diesem Zusammenhang soll zudem ein **Arbeitnehmerdatenschutzgesetz**[12] und ein **Informationszugangsgesetz** auf den Weg gebracht werden.

Zur Vorbereitung der zweiten Stufe der Novellierung des gesamten Datenschutzrechtes hat das Bundesinnenministerium einen Gutachterausschuss[13] beauftragt. Ergebnisse einer Voruntersuchung zu dem noch zu erstellenden Gutachten liegen vor[14].

Änderungen des BDSG im Überblick

Im neuen BDSG wurde nur eine nach der EG-Richtlinie zwingend erforderliche Anpassung vorgenommen, wobei der Entwurf an dem vertrauten – aber keineswegs übersichtlichen – Aufbau des BDSG weitgehend festhält. Weiterhin wird im BDSG entgegen der Vorgabe der EG-Richtlinie die **Trennung zwischen öffentlichen und nicht-öffentlichen Bereich** beibehalten, sodass das BDSG sowohl für den öffentlichen Bereich des Bundes, als auch für den nicht-öffentlichen Bereich (Privatbetriebe) gilt. Für die öffentlichen Stellen der Länder werden weiterhin die jeweiligen – und zum großen Teil noch zu novellierenden – Landesdatenschutzgesetze gelten. Die nachfolgend aufgezeigten Veränderungen im BDSG werden auch in den Landesdatenschutzgesetzen ihren Niederschlag finden müssen.

Dadurch, dass die Trennung zwischen öffentlichen und nicht-öffentlichen Bereich weiterhin aufrechterhalten wird, bleibt die Regelung in § 12 Abs. 4 BDSG für Arbeitnehmerdaten im öffentlichen Bereich des Bundes von Bedeutung. So unterliegen personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse den gleichen Vorgaben wie die Daten von Beschäftigten in den nicht-öffentlichern Stellen (Privatbetrieben)[15]. In bezug auf den Arbeitnehmer-Datenschutz gelten also für den öffentlichen Bereich des Bundes weitgehend die gleichen Vorgaben wie in Privatbetrieben oder Vereinen. Was also Nachfolgend für die nicht-öffentlichen Stellen gesagt wird, gilt weitgehend für den Arbeitnehmer-Datenschutz im öffentlichen Bereich des Bundes. Als wichtige Änderungen im BDSG sind folgende Vorschriften zu sehen:

- Anwendungsbereich – § 1 BDSG
- Begriffsbestimmungen – § 3 BDSG
- Datenvermeidung und Datensparsamkeit – § 3 a BDSG
- Übermittlung personenbezogener ins Ausland – §§ 4 b und 4 c BDSG
- Beauftragter für den Datenschutz – §§ 4 f und 4 g BDSG
- automatisierte Einzelentscheidungen – § 6 a BDSG
- Videoüberwachung – § 6 b BDSG
- Mobile personenbezogene Speicher- und Verarbeitungsmedien – § 6 c BDSG
- Schadensersatz – § 7 BDSG
- Technische und organisatorische Maßnahmen – § 9 BDSG
- Datenschutzaudit – § 9 a BDSG
- Widerspruchsrecht – § 35 BDSG
- Aufsichtsbehörde – § 38 BDSG.

Die neuen Regelungen im Einzelnen

Die notwendigsten Änderungen sind in die bestehende Struktur des BDSG und vor allem in den ersten Abschnitt eingeschoben worden, sodass beispielweise der § 4 BDSG um die § 4 a bis 4 g BDSG anwachsen wird.

Anwendungsbereich

Wie bereits erwähnt, nimmt das BDSG entgegen der DRL die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Bereich vor. So gilt der erste, vierte und fünfte Abschnitt des BDSG wie bisher für den öffentlichen und den nicht-öffentlichen Bereich, der zweite Abschnitt allein für den öffentlichen Bereich des Bundes und der dritte Abschnitt für den nicht-öffentlichen Bereich. Der sachliche Anwendungsbereich erstreckt sich auf die automatisierte Verarbeitung und teilweise auf die nicht-automatisierte Datenverarbeitung. Das BDSG gilt für den nicht-öffentlichen Bereich für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, soweit sie Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht-automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Während bisher die geschäftsmäßige Datenverarbeitung in oder aus Dateien erfolgen musste, reicht jetzt das Kriterium der automatisierten Verarbeitung personenbezogener Daten aus, um die Anwendung des BDSG auszulösen. Der Dateibezug bleibt lediglich bei nicht-automatisierter (also manueller) Verarbeitung erhalten. Ausgenommen vom Anwendungsbereich ist die Erhebung, Verarbeitung und Nutzung von Daten, die ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.

Die in § 1 Abs. 3 BDSG (alt) enthaltenen Ausnahmen für automatisierte Dateien, die ausschießlich aus verarbeitungstechnischen Gründen vorübergehend erstellt werden und für nicht-automatisierte Dateien, deren Daten nicht zur Übermittlung bestimmt sind, entfallen mit der Novellierung. So wird der Anwendungsbereich ausgeweitet.

§ 1 Abs. 5 BDSG setzt die in Art. 4 DRL über die Anwendung des jeweils anzuwendenden nationalen Datenschutzrechts um. Danach findet das BDSG keine Anwendung, sofern eine in einem anderen EU-Mitgliedstaat gelegene verantwortliche Stelle (im alten BDSG „speichernde Stelle" genannt) personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Erfolgt die Erhebung, Verarbeitung

11) Tauss/Özdemir, Umfassende Modernisierung des Datenschutzrechts in zwei Stufen, RDV 2000, S. 144.

12) Die Bundesregierung will bis 2002 ein seperates Arbeitnehmerdatenschutzgesetz auf den Weg bringen. Vgl. Handelsblatt v. 16. 10. 2000, S. 6; vgl. hierzu auch: Däubler, Ein Gesetz über den Arbeitnehmerdatenschutz, RDV 1999, S. 243 ff.

13) Der Gutachterausschuss besteht aus: Prof. Dr. Alexander Roßnagel, Prof. für Öffentl. Recht, Universität GH Kassel, Prof. Dr. Andreas Pfitzmann, TU Dresden und Prof. Dr. Hansjürgen Garstka, Berliner Beauftragter für den Datenschutz und Akteneinsicht.

14) Vgl. Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, DuD 2001, S. 253 ff.

15) Vgl. § 12 Abs. 4 BDSG: „Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse erhoben, verarbeitet oder genutzt, gelten anstelle der §§ 13 bis 16, 19 bis 20 der § § 28 Abs. 1 und 3 Nr. 1 sowie die §§ 33 bis 35, auch soweit personenbezogene Daten weder automatisiert verarbeitet noch in nicht-automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden."

und Nutzung jedoch durch eine Niederlassung des in der EU-ansässigen Staates ist das BDSG anzuwenden. Die Gesetzesbegründung[16] verweist in Bezug auf den Begriff „Niederlassung" auf § 42 Abs. 2 Gewerbeordnung. Dieser zufolge ist eine Niederlassung vorhanden, wenn der Gewerbetreibende eine zum dauernden Gebrauch eingerichteten, ständig oder in regelmäßiger Weise von ihm benutzten Raum für den Betrieb seines Gewerbes besitzt. Dieses beseutet, dass die Schwelle zur Annahme einer Niederlassung nicht besonders hoch ist, andererseits sind Zurechnungsprobleme in der Praxis nicht auszuschließen[17].

In § 1 Abs. 5 BDSG wird zudem klargestellt, dass die Zuständigkeit der Aufsichtsbehörden, auch wenn im Einzelfall EU-ausländisches Datenschutzrecht zur Anwendung kommt, unberührt bleibt. Das BDSG findet in jedem Fall Anwendung, wenn eine außerhalb der EU gelegene verantwortliche Stelle personenbezogene Daten in der Bundesrepublik Deutschland erhebt, verarbeitet oder nutzt.

Begriffsbestimmungen

§ 3 Abs. 2 BDSG enthält entsprechend der Vorgabe der DRL (Art. 3 Abs. 1 DRL) zwei neue Definitionen. Zum einen wird der Begriff der **„automatisierten Datenverarbeitung"**, zum andern der Begriff der **„nicht-automatisierten Datei"** definiert. „Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen." „Eine nicht-automatisierte Datei ist jede nicht-automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann." Somit ist das Kriterium der Datei für die Frage des sachlichen Anwendungsbreiches des Bundesdatenschutzgesetzes nur noch von Bedeutung, soweit es um nicht-automatisierte Erhebung, Verarbeitung und Nutzung personenbezogener Daten geht. Das Kriterium der nicht-automatisierten Datei hat zur Folge, dass **Akten** aus dem Anwendungsbereich des BDSG weitgehend ausgeschlossen bleiben. Zudem unterliegen dem BDSG zukünftig Bild- und Tonträger dem BDSG, denn sie stellen in der Regel automatisierte Verarbeitung personenbezogener Daten dar[18].

In § 3 Abs. 6 a BDSG wird der Begriff des **Pseudonymisieren** in das BDSG aufgenommen. „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." Grundsätzlich bringt die Anwendung von Pseudonymen jedoch die Möglichkeit mit sich, den Personenbezug wieder herzustellen. Somit ist das Anonymisieren, das ebenfalls nach dem BDSG als eine Maßnahme des Datenschutzes vorgesehen ist, das datenschutzfreundlichere Vorgehen[19]. Die Definition „Pseudonymisieren" kommt besondere Bedeutung im Zusammenhang mit der in § 3 a BDSG verankerten Vorgabe der Datenvermeidung und Datensparsamkeit zu.

In § 3 Abs. 7 BDSG wird anstelle des Begriffs der „speichernden Stelle" der Begriff der **„verantwortlichen Stelle"** eingeführt. „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt." Verpflichtungen aus dem Datenschutzrecht treffen demnach nicht mehr denjenigen, der – wie nach § 3 Abs. 8 BDSG „speichernde Stelle" genannt – einen technischen Vorgang ausführt, sondern die (natürliche oder juristische) Person, die über die Zwecke und Mittel der Verarbeitung entscheidet[20].

Neu in das BDSG aufgenommen sind in § 3 Abs. 9 BDSG besondere Arten personenbezogener Daten, die in der Literatur als **„sensitive" Daten** bezeichnet werden. „Besondere Arten personenbezogener Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben". Nach bisherigem deutschen Datenschutzverständnis gibt es keine Daten, die für sich genommen besonders „sensitiv" sind. Ausschlaggebend ist immer der Zusammenhang, in dem das personenbezogene Datum steht oder genutzt wird. So können durchaus vermeintlich harmlose Daten in Verbindung mit anderen Daten eine besondere Sprengkraft erlangen. Nach dem neuen BDSG unterliegen diese sensitiven Daten jedoch einem besonderen Schutz dahingehend, dass die Erhebung, Verarbeitung und Nutzung dieser Daten der ausdrücklichen Einwilligung des Betroffenen bedarf. Durch die Vorgabe der DRL ist die Regelung im BDSG zu den sensitiven Daten recht eigenwillig: „Denn bereits das BDSG beruht ja auf dem grundsätzlichen Verbot der Verarbeitung personenbezogener Daten. Diese ist bekanntlich nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder eine Einwilligung des Betroffenen vorliegt. Für sensitive Daten besteht daher sozusagen ein doppeltes Verbot mit Erlaubnisvorbehalt."[21]

Da in § 6 c BDSG eine Regelung zum Einsatz **mobiler personenbezogener Speicher- und Verarbeitungsmedien** enthält, ist in § 3 Abs. 10 BDSG eine Definition dahingehend enthalten, dass mobile personenbezogene Speicher- und Verarbeitungsmedien Datenträger sind,

- die an den Betroffenen ausgegeben werden,
- auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende Stelle automatisiert verarbeitet werden können und
- bei denen der Betroffene die Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Datenvermeidung und Datensparsamkeit

Nach § 3 a BDSG haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Der **Grundsatz der Datenvermeidung** und **Datensparsamkeit** wird erstmalig in das BDSG aufgenommen. Die Vorschrift konkretisiert den Grundsatz der Verhältnismäßigkeit für

16) Vgl. die Gesetzesbegründung: Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze, Synopse zu dem am 23. Mai 2001 in Kraft tretenden Änderungen (nur) des BDSG (mit Begündung des Regierungsentwurfs, BT-Drs. 14/4329, und Begründung zur Beschlussempfehlung des BT-Innenausschusses vom 4. 4. 2001, BT-Drs. 14/5793, herausgegeben vom Bundesministerium des Inneren, Referat V 7, S. 13 f.

17) Vgl. Christians, Das neue Bundesdatenschutzgesetz: Die Änderungen im Überblick, Datenschutz Nachrichten 4/2000, S. 15.

18) Vgl. Christians, (Fn. 17), S. 10.

19) Vg. hierzu ausführlich: Arbeitskreis Technik der Datenschutzbeauftragten, Datenschutzfreundliche Technologien, DuD 1997 S. 709 ff.

20) Vgl. Brühann/Zerdick, (Fn. 4), S. 430.

21) Christians, (Fn. 17), S. 16.

die technische Gestaltung der Datenverarbeitungssysteme. Eine vergleichbare Regelung findet sich in § 3 Abs. 4 des Teledienstedatenschutzgesetzes. Wie dort soll durch die Einführung des Grundsatzes bereits durch die Gestaltung der Systemstrukturen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten möglichst gering gehalten werden. So sollen Eingriffe für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein vermieden werden[22].

Bei bargeldloser Zahlung in der Betriebskantine entsprechen Kantinenabrechnungssysteme, die so angelegt sind, dass der zu zahlende Betrag im Rahmen der Lohn- und Gehaltsabrechnung vom Lohn/Gehalt abgezogen wird, nicht der Vorgabe der Datenvermeidung und Datensparsamkeit. Dahingegen wird ein Kantinenabrechnungssystem, bei dem der Beschäftigte seine Magnet- oder Chipkarte an einem Automaten mit einem Geldbetrag aufgeladen kann und dann bei der Bezahlung ein entsprechender Geldbetrag von der Karte abgebucht wird, der Vorgabe der Datenvermeidung und Datensparsamkeit eher gerecht, da keine personenbezogenen Daten der Beschäftigten verarbeitet werden.

§ 3 a Satz 2 BDSG beinhaltet den Vorrang anonymer und pseudonymer Formen der Datenverarbeitung als eine von mehreren Möglichkeiten der Ausgestaltung des Systemdatenschutzes als ein Mittel dem Grundsatz der Erforderlichkeit der Datenverarbeitung Rechnung zu tragen.

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

Das novellierte BDSG geht auch weiterhin von einen **Verarbeitungsverbot mit Erlaubnisvorbehalt** aus. Dabei wird die Erhebung von Daten auch diesem Regelungsprinzip unterworfen. Im alten BDSG war lediglich eine Erhebung nach Treu und Glauben verankert (§ 28 Abs. 1 BDSG-alt). D. h. die Datenerhebung, -verarbeitung und -nutzung ist nur zulässig, soweit

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

Diese Neuregelung wird zur Folge haben müssen, dass **alle eingesetzten Personalfragebogen,** die im Rahmen von Einstellungen genutzt weden, **überprüft** werden müssen.

Zusätzlich wird in § 4 Abs. 2 BDSG festgelegt, dass die Erhebung von Daten beim Betroffenen selbst zu erfolgen hat; es wird also das **Prinzip der Direkterhebung** verankert. Durch diese Regelung bekommt der Rechtsgedanke, der bereits in § 13 Abs. 2 BDSG (alt) für den öffentlichen Bereich des Bundes verankert ist, auch für Privatbetriebe Bedeutung. Dieser Grundsatz, dass personenbezogene Daten beim Betroffenen direkt zu erheben sind, ist unmittelbarer Ausfluss des Volkszählungsurteils und des informationellen Selbstbestimmungsrechts. Der Betroffene soll wissen, wer wann welche Daten über ihn sammelt, speichert und verarbeitet. Im Grundsatz sind personenbezogene Daten beim Betroffenen selbst und nicht hinter seinem Rücken zu erheben. „Beim Betroffenen" bedeutet, dass die Daten mit seiner **Kenntnis oder Mitwirkung** erhoben werden.

Zudem muss die verarbeitende Stelle zum Zeitpunkt der Erhebung eine konkrete Festlegung der Verarbeitszwecke vornehmen.

Der Gesetzesentwurf sieht jedoch Ausnahmen dahingehend 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
- die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde.

Diese Ausnahmen kommen aber nur dann zum Tragen, wenn keine Anhaltspunkte dafür bestehen, dass das überwiegende Schutzinteresse des Betroffenen beeinträchtigt wird.

In § 4 Abs. 3 BDSG 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 an diese rechnen muss.

Soll als Rechtsgrundlage der Datenerhebung, -verarbeitung oder -nutzung auf das BDSG selbst zurückgegriffen werden, bildet der § 28 BDSG weiterhin die rechtliche Basis. Eine der wesentlichen Änderungen besteht in der Einbeziehung der Erhebungsphase. D. h. die Erhebung von Beschäftigen- oder Bwerberdaten darf – wie bereits die Verarbeitung und Nutzung – nur in einer sehr engen Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses erfolgen.

Zusätzlich sind bereits bei der Erhebung die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Einwilligung

Die Einwilligung als eine mögliche Basis für die rechtmäßige Datenerhebung, -verarbeitung oder -nutzung ist in einem gesonderten Paragraphen geregelt. Die im aktuellen BDSG verankerten Vorgaben wie die **Schriftform** wurden beibehalten. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Zusätzlich muss die Einwilligung auf der „freien Entscheidung des Betroffenen" beruhen. Für die sensitiven Daten schreibt § 4 a Abs. 3 BDSG vor, dass sich eine entsprechende Einwilligung sich „ausdrücklich" auf diese Daten beziehen muss.

Andere Rechtsvorschrift

Weiterhin kann sich eine verantwortliche Stelle, die rechtmäßig Datenerhebung, -verarbeitung und -nutzung betreiben will, neben den Möglichkeiten eine Einwilligung einzuholen oder sich auf das BDSG (§ 28 BDSG) selbst zu stützen, auf eine **andere Rechtsvorschrift** beziehen. Eine andere Rechtvorschrift in diesem Sinne stellt weiterhin eine **Dienst- oder Betriebsvereinbarung** dar.

Übermittlung personenbezogener Daten ins Ausland

Zu den für die Praxis bedeutsamen Neuerungen infolge der DRL gehören die

22) Vgl. Gesetzesbegründung (Fn. 16) zu § 3 a BDSG.

Vorgaben zum grenzüberschreitenden Datenverkehr. Bisher gab es im BDSG keine eigenständige Regelung für die Übermittlung von Daten ins Ausland. Die Richtline sieht eine differenzierte Regelung vor, die auch für den öffentlichen Bereich gilt. Innerhalb der Mitgliedstaaten der Europäischen Union sieht die DRL den „freien Datenverkehr" vor. Vor diesem Hintergrund stellt § 4 b Abs. 1 BDSG den innergemeinschaftlichen dem inländischen Datentransfer gleich. So ist ein Datentransfer von München nach Paris künftig genauso zu behandeln wie ein Datentransfer von München nach Hamburg. Für die Übermittlung der Daten gelten die in § 4 i.V.m. § 28 BDSG enthaltenen Zulässigkeitsvoraussetzungen.

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 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 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 aufwendig sein. Deshalb sieht Art. 25 Abs. 6 DRL vor, dass die EU-Kommission für ein Drittland allgemein die Feststellung in Bezug auf ein angemessenes Datenschutzniveau treffen kann. Entsprechendes gilt für den umgekehrten Fall, wenn ein angemessenes Datenschutzniveau nicht besteht. Positive Feststellungen wurden zwischenzeitlich für Ungarn und die Schweiz getroffen.

Im Fall der 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")[23] für die Daten aus Europa vereinbart worden. US-Unternehmen können sich freiwillig den Regeln des „Safe Harbors" unterwerfen und sind dann 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-Handelministerium davon zu überzeugen, dass ihr Geschäftpartner dem „Safe Harbor" angehört.

Auch wenn ein Empfängerland kein angemessenes Datenschutzniveau gewährleistet, lässt § 4 c BDSG **Ausnahmen** zu, wie z. B. die **Einwilligung durch den Betroffenen.** Darüberhinaus 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.

Soll beim Datentransfer von Beschäftigtendaten mit einer Einwilligungserklärung gearbeitet werden, stellt die Einwilligungserklärung einen mitbestimmungspflichtigen Personalfragebogen im Sinne des § 94 BetrVG/§ 75 Abs. 3 Nr. 8 BPersVG dar, denn das Mitbestimmungsrecht deckt auch die Fälle ab, in denen der Beschäftigte nur nach einer einzigen Sache gefragt wird[24].

Meldepflicht

Automatisierte Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen Stellen der Aufsichtsbehörde zu melden. Eine entsprechende Meldepflicht gilt für öffentliche Stellen gegenüber dem **Bundesbeauftragten für den Datenschutz**. Die deutsche Delegation in Brüssel hat mit Erfolg darauf hingewiesen, dass aus deutscher Sicht im Bereich der Privatwirtschaft ein zur staatlichen Aufsicht mindestens gleichwertiger Datenschutz durch eine qualifizierte Eigenkontrolle durch die Bestellung eines betrieblichen Datenschutzbeauftragten gewährleistet werden kann. So enthält die DRL und auch das BDSG einen Passus dahingehend, dass eine Meldepflicht entfällt, „wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat." (§ 4 d Abs. 2 BDSG)

Eine Meldepflicht und auch die Bestellung eines betrieblichen Datenschutzbeauftragten entfällt für Kleinbetriebe, bei denen lediglich vier Arbeitnehmer personenbezogene Daten erheben, verarbeiten oder nutzen. Diese Ausnahme entspricht nicht den Vorgaben der DRL.

Der Inhalt der Meldepflicht wird in § 4 e BDSG festgelegt. Im Rahmen der Meldepflicht sind 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.

Vorabkontrolle

Über die ohnehin vorgegebene Zulässigkeitsprüfung nach § 4 i.V.m. § 28 BDSG hinaus ist bei Datenverarbeitung mit besonderen Risiken für den Betroffe-

23) Vgl. Die Safe-Harbor-Grundsätze, RDV 2000, S. 228 ff.; Möller, Gar nichts muss der Müller tun, Online-Marketing, Safe Harbor Principles und Strategien für den Datenschutz, Datenschutz Nachrichten, 2/2000, S. 15; Schierbaum, Grenzüberschreitender Datentransfer, Computer Fachwissen, 1999, S. 36 ff.

24) Vgl. Däubler, Grenzüberschreitender Datenschutz, AiB 1997, S. 259 ff.

nen eine Vorabkontrolle durchzuführen (§ 4 d Abs. 5 und 6 BDSG)[25]. Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen diese der Prüfung vor Beginn der Verarbeitung. Das Gesetz nennt Beispiele dafür, wann eine Vorabkontrolle durchzuführen ist. Eine **Vorabkontrolle** ist **insbesondere** dann durchzuführen, wenn

- besondere Arten personenbezogener 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.

In beiden Fällen ist die Vorabkontrolle nur dann durchzuführen, wenn der Verarbeitung weder eine gesetzliche Verpflichtung noch eine Einwilligung zugrunde liegt und sie auch nicht im Rahmen eines Vertragsverhältnisses erfolgt. Zuständig für die Vorabkontrolle ist gemäß § 4 d BDSG der Beauftragte für den Datenschutz. Der Beauftragte für den Datenschutz hat sich in Zweifelsfällen in Bezug auf die Vorabkontrolle an die Aufsichtsbehörde zu wenden.

Beauftragter für den Datenschutz

Die Vorschriften über den Datenschutzbeauftragten und seine Aufgaben wurden in den allgemeinen Teil des Gesetzes (Abschnitt 1) übernommen. Für den öffentlichen Bereich des Bundes stellt dieses eine Neuerung dar, da bisher für diesen Bereich keine gesetzlichen Vorschriften bestanden[26]. Die Bestellung eines **Datenschutzbeauftragten** ist somit sowohl für den **öffentlichen Bereich** als auch den nicht-öffentlichen Bereich **verpflichtend**. Weiterhin sind Kleinbetriebe von der Bestellung eines betrieblichen Datenschutzbeauftragten freigestellt. Denn die Bestellung eines Datenschutzbeauftragten muss nur dann erfolgen, wenn mehr als vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind (§ 4 f Abs. 1 BDSG). Eine entsprechende Ausnahme ist nach der DRL nicht vorgesehen, wird aber vom bundesdeutschen Gesetzgeber weiterhin eher willkürlich vorgenommen und ist allenfalls von dem Bemühen getragen, Kleinbetriebe von zusätzlichen Organisationspflichten zu befreien. Grundsätzlich hängt die Gefährdung der Persönlichkeitsrechte nicht allein von der Zahl der Beschäftigten ab. So kann davon ausgegangen werden, dass nur eine Person an einem entsprechend ausgestatteten PC erheblich mehr anfangen kann als eine Bedienermannschaft von zwanzig Mitarbeitern in einem Rechenzentrum der siebziger Jahre, also zu der Zeit in der die Ausnahmeregelung entstanden ist.

In Bezug auf die Person des **betrieblichen/behördlichen Datenschutzbeauftragten,** deren persönlichen Voraussetzungen, dem verankerten Benachteiligungsverbot und auch der zu erfüllenden Aufgaben hat sich gegenüber den Vorgaben der §§ 36 bis 37 BDSG (alt) nichts Grundlegendes verändert. Der Gesetzgeber hat es insbesondere versäumt, ein Beteiligungsrecht der Interessenvertretungen oder auch einen besonderen Kündigungsschutz des betrieblichen Datenschutzbeauftragten zu verankern. Es ist nicht nachzuvollziehen, warum hier gerade in diesen Punkten eine Gleichstellung mit den Beauftragten im Bereich des Umweltrechtes (wie z. B. Immissionsschutzbeauftragter, Störfallbeauftragter, Abfallbeauftrager)[27] nicht mit der Novellierung des BDSG erfolgt ist.

Mit dem neuen BDSG kommen auf den betrieblichen/behördlichen Datenschutzbeauftragten **zwei neue Aufgaben** zu:

Erstens muss der betriebliche Datenschutzbeauftragte gemäß § 4 d Abs. 5 BDSG die Vorabkontrolle durchführen. Und **zweitens** hat der betriebliche Datenschutzbeauftragte in den Fällen, in denen keine Meldepflicht besteht, auf Antrag jedermann die gemäß § 3 g Abs. 2 BDSG 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).

Eine weitere Neuerung besteht darin, dass datenverarbeitende 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 (§ 4 f Abs. 1 BDSG).

Automatisierte Einzelentscheidungen

Der § 6 a BDSG stellt die Umsetzung der Vorgabe des Art. 15 DRL dar und ist insoweit eine Besonderheit, als nicht die Zulässigkeit der Datenverarbeitung selbst geregelt wird, sondern Entscheidungsabläufe reguliert werden. Nach § 6 a Abs. 1 BDSG dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der **Bewertung einzelner Persönlichkeitsmerkmale** dienen. Der Grundgedanke der Vorschrift des Art. 15 DRL ist dem französischen Recht entnommen und erforderte numehr die ausdrückliche Aufnahme in das BDSG. Durch die Vorschrift wird die Zulässigkeit von Entscheidungen eingeschränkt, die auf der Basis bestimmter automatisierter Datenverarbeitung getroffen werden. Die Vorschrift beruht auf dem Grundgedanken, dass Entscheidungen, die die Bewertung einer Person beinhalten und daher das Persönlichkeitsrecht zentral berühren, nicht einem Computerprogramm überlassen werden dürfen[28].

§ 6 a Abs. 2 BDSG enthält **Ausnahmen** zu dem verankerten Verbot. Es gilt nicht, wenn

- die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
- 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 ist ein besonderes **Auskunftsrecht** dahingehend verankert, das sich bei automatisierten Ent-

25) Vgl. Schild, Meldepflichten und Vorabkontrolle, DuD 2001, S. 282 ff.

26) Vgl. zum betrieblichen/behördlichen Datenschutzbeauftragten: Schierbaum, Der behördliche Datenschutzbeauftragte – eine obligatorische Institution mit der Umsetzung der EG-Datenschutzrichtlinie, PersR 1998, S. 259 ff.; Schierbaum/Kiesche, Der betriebliche Datenschutzbeauftragte, CR 1992, S. 726 ff.

27) Vgl. hierzu: Schierbaum/Nahrmann, Betriebsbeauftragte für den Umweltschutz, AiB 1997, S. 36 ff.

28) Vgl. Dammann/Simitis, (Fn 2), Art. 15 Anm. 1.

scheidungen auch auf den logischen Aufbau der automatisierten Verarbeitungen der der betreffenden personenbezogenen Daten bezieht. D. h. in diesen Fällen wird das in § 34 und § 19 BDSG verankerte Auskunftsrecht auch auf den Verarbeitungsvorgang selbst ausgeweitet. Die Probleme für die praktische Umsetzung dieser Vorgabe sind jedoch nicht zu übersehen, da die Softwareprogramme heute angesichts der rückläufigen Preise für Speicherkapazität meist äußerst umfangreich und komplex sind. In jedem Fall muss der logische Aufbau, so wie er sich im Programmablauf vollzieht, der betroffenen Person verständlich gemacht werden, so dass die betroffenen Person verstehen kann, in welcher Weise aus ihren konkreten personenbezogenen Daten bestimmte Bewertungen oder Klassifizierungen abgeleitet werden und welche Bedeutung diese Werte im Verarbeitungssystem besitzen[29].

Videoüberwachung

In § 6b BDSG wird erstmals eine Rechtsgrundlage zur Videoüberwachung geschaffen. So ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke zulässig und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Vorschrift erfaßt nur öffentlich zugängliche Räume wie etwa Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhalten.

In der Gesetzesbegründung[30] heißt es, dass für nicht öffentlich zugängliche Räume besondere Regelungen, beispielsweise im Rahmen eines Arbeitnehmerdatenschutzgesetzes, erorderlich sind. Dieses kann in der Praxis zu Irritationen führen. Denn aus der Gesetzesbegründung könnte durchaus der Schluss gezogen werden, dass Betriebe mit Videoüberwachung diese bis zu einer gesetzlichen Regelung einstellen müßten. Man wird wohl davon ausgehen müssen, dass die Zulässigkeit von Videoüberwachung in nicht öffentlich zugänglichen Räumen den Vorgaben der § 4 i. V. m. § 28 BDSG unterliegen.

Bei Videoüberwachung in öffentlich zugänglichen Räumen dient die Regelung in § 6b Abs. 2 BDSG der Transparenz. Denn der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Geeignete Maßnahmen können deutlich sichtbare Hinweisschilder sein, auf denen der Umstand der Videoüberwachung und auch die verantwortliche Stelle erkennbar ist.

Werden durch die Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend der §§ 19a und 33 BDSG zu benachrichtigen.

Zusätzlich enthält § 6b Abs. 5 BDSG eien Vorgabe zur Löschung von Video-Daten. So sind Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Mobile personenbezogene Speicher- und Verarbeitungsmedien

Der § 6c BDSG enthält vor allem ein **Recht auf Unterrichtung** des Betroffenen beim Einsatz von mobilen Speichermedien. Zu diesen Speichermedien gehören z. B. Chip- oder Magnetkarten. Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat. Die Auskunft muss folgende Aspekte umfassen:

- die Identität und Anschrift der Stelle,
- in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
- Informationen, wie der Betroffene seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung ausüben kann und
- über die bei Verlust und Zerstörung des Mediums zu treffenden Maßnahmen.

Zusätzlich müssen Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, für den Betroffenen eindeutig erkennbar sein (§ 6c Abs. 3 BDSG).

Schadensersatz

In § 7 BDSG-E wird die Reglung des Art. 23 DRL umgesetzt und erstmals im Bundesdatenschutzgesetz eine eigenständige Anspruchsgrundlage für die Haftung geschaffen, die sowohl für die öffentlichen und 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 ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht soll entfallen, soweit die verantwortliche Stelle die nach den Umständen des Falles die gebotene Sorgfalt beachtet hat.

Technische und organisatorische Maßnahmen

Die in § 9 BDSG vorgegebenen Datenschutz- und Datensicherungsmaßnahmen bleiben auch im neuen BDSG bestehen. Die Anlage zu § 9 BDSG wird jedoch inhaltlich veändert und von zehn auf acht Zielvorgaben gekürzt. Die folgenden Zielvorgaben sind bei der Verarbeitung personenbezogener Daten zwingend einzuhalten:

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 unterliegen-

29) Vgl. Dammann/Simitis, (Fn 2), Art. 12 Anm. 4.

30) Vgl. Gesetzesbegründung (Fn. 16) zu § 6b BDSG.

den 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 des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft 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 festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verädert und 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.

Neu in das BDSG aufgenommen worden ist die Vorgabe der „**Getrennten Verarbeitung**". Das Trennungsgebot stellt in technischer Hinsicht klar, was von der rechtlichen Seite in Bezug auf die enge Zweckbindung der Datenverarbeitung ohnehin vorgesehen ist. Eine ähnliche, aber speziellere Bestimmung enthält bereits das Teledienstedatenschutzgesetz im Hinblick auf zu unterschiedlichen Zwecken erhobene Daten eines Nutzers von Telediensten[31].

Datenschutzaudit

Die Regelung zum Datenschutzaudit[32] entspricht dem § 17 Mediendienste-Staatsvertrag der Länder. Nach § 9a BDSG können Anbieter von Datenverarbeitungsystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtugnen durch unabhängige Gutachter prüfen und bewerten lassen[33]. 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 § 9a BDSG durch ein Gesetz geregelt werden.

Widerspruchsrecht

In § 35 Abs. 5 BDSG werden die Benachrichtungs- und Auskunftsrechte um ein Widerspruchsrecht ergänzt. Es wird Art. 14 DRL umgesetzt, sodass der Betroffene in den Datenverarbeitungsprozess dahingehend eingreifen kann, die Verarbeitung – auch im Falle ihrer Rechtmäßigkeit – zu untersagen. Das Widerspruchrecht greift ein, soweit der Betroffene der Datenverarbeitung bei der verantwortliche Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation 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 Widerspruchtsrecht im Arbeitsleben zum Tragen kommen kann, ist sehr fraglich.

Aufsichtsbehörde

Die wichtigste Veränderung für die Praxis ist der **Wegfall** der sogenannten **Anlasskontrolle**. Nach dem bisherigen BDSG konnte die Aufsichtsbehörde dann tätig werden, wenn ihr hinreichende Anhaltspunkte vorliegen, dass eine nicht-öffentliche Stelle gegen Datenschutz-Vorschriften verstoßen hat oder der Betroffene einen Verstoß begründet darlegt. Nach dem novellierten Bundesdatenschutzgesetz kann die Aufsichtsbehörde **jederzeit** tätig werden.

Datenschutz durch Mitbestimmung

Ein wichtiges Regelungsinstrument mit langer Tradition für die Zulässigkeit der Verarbeitung von Beschäftigtendaten stellen **Betriebs-/Dienstvereinbarungen** dar, die als übergreifende Rahmenvereinbarungen oder als Einzelvereinbarungen detaillierte Regelungen zum Arbeitnehmerdatenschutz enthalten. Entsprechende Regelungen werden insbesondere in Ausübung des Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG/§ 75 Abs. 3 Nr. 17 BPersVG getroffen. Dabei gehen auch weiterhin mit der Novellierung des BDSG Betriebs-/Dienstvereinbarungen als „andere Rechstvorschriften" im Sinne des § 4 Abs. 1 BDSG dem Datenschutzgesetz vor, sodass diese Vereinbarungen in ihrem Regelungsbereich das BDSG verdrängen.

In keinem Fall dürfen jedoch Betriebs-/Dienstvereinbarungen schlechtere Regelungen enthalten als das BDSG. Und natürlich verändert sich mit der Novellierung des BDSG 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 nach § 94 BetrVG/§ 75 Abs. 3 Nr. 8 BPersVG bei Personalfragebogen die Einbeziehung der Erhebung in § 4 BDSG und der damit verbundenen engeren Zulässigkeit der Erhebung von Daten zu berücksichtigen sein. In jedem Fall müssen Betriebs-/Personalräte an Schulungen zur neuen Rechtslage teilnehmen können.

Bruno Schierbaum, BTQ Niedersachsen,
Donnerschweer Str. 84,
26123 Oldenburg
e-mail: schierbaum@btq.de

31) Vgl. Christians, (Fn. 17) S. 22.

32) Vgl. zum Datenschutzaudit: Roßnagel, Datenschutzaudit – Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit – Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie, Kassel im Mai 1999; verfügbar im Internet unter http://www.iukdg.de; vgl. auch Wedde/Schröder, Qualität im Datenschutz-quid, AiB 2001, S. 284 ff.

33) Vgl. hierzu Roßnagel, Datenschutzaudit – Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit – Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie, 1999 (im Internet unter: www.iukdg.de).