Deutscher Bundestag
13. Wahlperiode

Drucksache 13/9082

14. 11. 97

Sachgebiet 204

Gesetzentwurf

des Abgeordneten Manfred Such und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Bundesdatenschutzgesetzes (BDSG)

A. Problem

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-DSRL) verlangt bis Oktober 1998 eine grundlegende Überarbeitung des nationalen Datenschutzrechts. Außerdem hat sich gezeigt, daß das seit 1990 geltende Datenschutzgesetz nicht in der Lage ist, angesichts neuer Entwicklungen der Informations- und Kommunikationstechnik einen ausreichenden rechtlichen Gestaltungsrahmen mit dem Ziel des angemessenen Schutzes des allgemeinen Persönlichkeitsrechts bzw. des Rechts auf informationelle Selbstbestimmung abzugeben. Die Erfahrungen mit dem BDSG lassen in zunehmendem Maße Vollzugsprobleme und Vollzugsdefizite erkennen. Die dafür ursächlichen Regelungsdefizite und damit die bestehende Rechtsunsicherheit sollen mit dem Gesetzentwurf behoben werden.

B. Lösung

Das BDSG wird bezüglich Terminologie, Struktur und Inhalt an die EU-DSRL angepaßt. Entsprechend der Forderung der Datenschutzbeauftragten des Bundes und der Länder werden die Vorschriften für den öffentlichen und den privaten Bereich mit dem Ziel eines hohen Schutzes der Betroffenen vereinheitlicht. Die Rechte der Betroffenen und die Transparenz der Datenverarbeitung werden ausgebaut. Das Instrument der Technikfolgenabschätzung wird eingeführt. Die Datenschutzkontrolle wird verbessert. Darüber hinaus werden u. a. folgende Vorschläge der Datenschutzbeauftragten umgesetzt:

- Erweiterung des Schutzbereichs, Regelung der Videoüberwachung,
- stärkere Einbeziehung von Presse und Medien,
- Sonderregelung für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten oder Gesundheitsdaten,

- Ausrichtung des Rechts auf die Gegebenheiten moderner Multimediaanwendungen (anonyme Nutzung, Datensparsamkeit),
- Regelung für Chipkartenanwendungen,
- Schutz bei Persönlichkeitsbewertungen durch den Computer,
- verbesserter Schutz gegenüber Adressenhandel und Direktmarketing,
- Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung.

C. Alternativen

Die Beschränkung der Novellierung des BDSG auf die Anpassung an die EU-DSRL würde kurzfristig eine erneute Novellierung nötig machen und die Rechtsunsicherheit erhöhen.

D. Kosten

Mit direkten zusätzlichen Kosten ist nicht zu rechnen. Die Vereinfachung des Rechts wird in einigen Bereichen zu Einsparungen führen. Neue datenschutzrechtliche Instrumente (z. B. Technikfolgenabschätzung, Führung von Widerspruchslisten beim Bundesbeauftragten) können gewisse Mehrkosten verursachen. Diese Maßnahmen ermöglichen jedoch zugleich Einsparungen bei den verarbeitenden Stellen.

Entwurf eines Bundesdatenschutzgesetzes (BDSG)

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Inhaltsübersicht

ERSTER ABSCHNITT

Allgemeine Bestimmungen

ERSTER UNTERABSCHNITT

Grundlagen

§ 1

Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist der Schutz der Grundrechte, insbesondere der Privatsphäre und des Rechts auf informationelle Selbstbestimmung, bei der Verarbeitung personenbezogener Daten.

(2) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch

1. öffentliche Stellen des Bundes und
2. nicht öffentliche Stellen, soweit diese personenbezogene Daten nicht ausschließlich für persönliche und private Zwecke verarbeiten und die Daten automatisiert oder in einer strukturierten Sammlung, die nach bestimmten Kriterien zugänglich ist, gespeichert werden, gespeichert werden sollen oder aus einer solchen Datensammlung stammen.

(3) Soweit eine Stelle, die ihren Sitz in einem anderen Mitgliedstaat der Europäischen Union hat, im Inland personenbezogene Daten verarbeitet und eine Niederlassung unterhält, sind die Vorschriften dieses Gesetzes anzuwenden. Dieses Gesetz findet auch Anwendung, soweit eine Stelle außerhalb der Europäischen Union personenbezogene Daten im Inland verarbeitet; in diesem Fall hat die verarbeitende Stelle einen im Inland ansässigen Vertreter zu benennen, dem die Rechte und Pflichten der verarbeitenden Stelle obliegen. Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union gelegene Stelle personenbezogene Daten im Inland verarbeitet, ohne daß sie im Inland eine Niederlassung unterhält. Es findet auch keine Anwendung, wenn die Verarbeitung nur dem Zweck der Durchfuhr durch das Gebiet der Europäischen Union dient.

(4) Soweit besondere Rechtsvorschriften des Bundes und der Europäischen Gemeinschaften die Verarbeitung personenbezogener Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor. Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit personenbezogene Daten verarbeitet werden.

§ 2

Öffentliche und nicht öffentliche Stellen

(1) Öffentliche Stellen sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstige der Aufsicht des Bundes oder eines Landes unterstehende Personen des öffentlichen Rechts sowie Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Öffentliche Stellen sind auch entsprechende Stellen in den Mitgliedstaaten der Europäischen Union sowie Stellen der Europäischen Union.

(2) Öffentliche Stellen sind auch juristische Personen und sonstige Vereinigungen des privaten Rechts, soweit den in Absatz 1 genannten Stellen die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

(3) Öffentliche Stellen des Bundes im Sinne dieses Gesetzes sind öffentliche Stellen nach den Absätzen 1 und 2, wenn

1. sie Einrichtungen des Bundes sind oder der Aufsicht des Bundes unterstehen,
2. sie regelmäßig über den Bereich eines Landes oder bestimmter Länder hinaus tätig werden oder
3. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

(4) Nicht öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 und 2 fallen. Als nicht öffentliche Stellen gelten öffentlich-rechtliche Religionsgesellschaften und Stellen in Staaten außerhalb der Europäischen Union. Nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3

Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person).

(2) Automatisiert ist eine Verarbeitung personenbezogener Daten, die unter Einsatz von elektronischen Datenverarbeitungssystemen durchgeführt wird.

(3) Verarbeiten (Verarbeitung) ist jeder Umgang mit personenbezogenen Daten und umfaßt das Erheben, Speichern, Nutzen, Übermitteln, Veröffentlichen, Verändern, Sperren und Löschen. Im einzelnen ist

1. Erheben das Beschaffen von Daten über die betroffene Person,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung,
3. Nutzen jede sonstige Verwendung personenbezogener Daten innerhalb der verarbeitenden Stelle einschließlich ihrer Weitergabe,
4. Übermitteln das Bekanntgeben oder sonstige Offenbaren personenbezogener Daten an Dritte, insbesondere durch Weitergabe an Dritte oder durch Einsichtnahme oder Abruf von hierzu bereitgestellten Daten,

5. Veröffentlichen das Übermitteln an eine unbestimmte Zahl von Dritten,
6. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
7. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um die weitere Verarbeitung einzuschränken,
8. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(4) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Angaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(5) Verarbeitende Stelle ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, unabhängig davon, ob sie die Daten selbst verarbeitet oder durch andere im Auftrag verarbeiten läßt.

(6) Dritter ist jede Person oder Stelle außerhalb der verarbeitenden Stelle. Dritte sind nicht die betroffene Person sowie diejenigen, die im Inland oder im Hoheitsgebiet eines anderen Mitgliedstaates der Europäischen Union personenbezogene Daten im Auftrag verarbeitet. Empfänger ist jede Person, die personenbezogene Daten erhält (Dritte als Übermittlungsempfänger und Auftragsdatenverarbeiter).

(7) Datenschutzkontrollinstanzen sind der Bundesbeauftragte für den Datenschutz sowie die Aufsichtsbehörden nach § 48.

§ 4
Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat.

§ 5
Einwilligung

(1) Einwilligung ist die widerrufliche, freiwillig und eindeutig bestimmbar abgegebene Willenserklärung einer betroffenen Person, einer bestimmten Datenverarbeitung zuzustimmen.

(2) Die Einwilligung bedarf der Schriftform, es sei denn, daß wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild hervorzuheben. Die betroffene Person ist auf den Zweck, Inhalt und Umfang der Verarbeitung hinzuweisen sowie, unter Darlegung der Folgen, daß sie die Einwilligung verweigern und widerrufen kann.

(3) Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, daß

1. sie nur durch eindeutige und bewußte Handlung der betroffenen Person erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. die Urheberschaft erkannt werden kann,
4. diese protokolliert wird und
5. deren Inhalt von der betroffenen Person jederzeit ohne unverhältnismäßigen Aufwand zur Kenntnis genommen werden kann.

§ 6
Datenerhebung

(1) Personenbezogene Daten sind bei der betroffenen Person zu erheben. Sie ist über die speichernde Stelle, den Zweck der Erhebung und die beabsichtigte weitere Verarbeitung sowie über eine zugrundeliegende Rechtsvorschrift aufzuklären. Soweit eine Auskunftspflicht besteht oder die Gewährung von Rechtsvorteilen die Angaben von Daten voraussetzt, ist die betroffene Person hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Die betroffene Person ist über die Empfänger oder Kategorien von Empfängern sowie über ihre Datenschutzrechte aufzuklären, soweit dies nicht auf Grund der Umstände unangemessen ist.

(2) Ohne Mitwirkung der betroffenen Person dürfen Daten nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. die erfüllende Aufgabe oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
3. die Erhebung bei der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen der betroffenen Person beeinträchtigt werden. Erfolgt die Erhebung über die betroffene Person bei einem Dritten, der nicht öffentliche Stelle ist, so ist dieser entsprechend Absatz 1 Satz 2 und 3 aufzuklären.

§ 7
Verantwortung bei der Datenübermittlung

Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Grund eines Ersuchens einer öffentlichen Stelle, so hat die übermittelnde Stelle lediglich zu prüfen, ob sich das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers hält. Die Rechtmäßigkeit prüft sie, wenn hierzu Anlaß besteht; der Empfänger hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen.

§ 8

Datenübermittlung in Drittländer

(1) Für die Übermittlung an Stellen außerhalb der Europäischen Union sowie an über- und zwischenstaatliche Stellen sind die für die Übermittlung geltenden Vorschriften anzuwenden, wenn im Drittland ein angemessenes Datenschutzniveau gewährleistet ist.

(2) Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände festgestellt, die bei der Datenübermittlung von Bedeutung sind. Herangezogen werden können insbesondere

- die Art der Daten,
- die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung,
- das Herkunfts- und das Bestimmungsland,
- die im Drittland geltenden Rechtsnormen, Standesregeln und Sicherheitsmaßnahmen.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt werden.

(4) Ist im Drittland kein angemessenes Datenschutzniveau gewährleistet, so steht dieser Umstand der Übermittlung nicht entgegen, wenn

1. die betroffene Person ihre Einwilligung erteilt hat,
2. die Übermittlung im Rahmen eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit der betroffenen Person erforderlich ist,
3. die Übermittlung zum Abschluß oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person von der verarbeitenden Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung eines rechtlichen Interesses erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist,
6. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt.

(5) Unbeschadet von Absatz 4 kann die zuständige Datenschutzkontrollinstanz eine Übermittlung oder eine Kategorie von Übermittlungen genehmigen, wenn die speichernde Stelle ausreichende Garantien hinsichtlich des Schutzes der in § 1 Abs. 1 genannten Grundrechte bietet; diese Garantien können sich aus Vertragsklauseln ergeben.

(6) Die Datenschutzkontrollinstanzen unterrichten die zuständigen Stellen der übrigen Mitgliedstaaten der Europäischen Union und der Europäischen Kommission über Drittländer ohne angemessenes Datenschutzniveau nach Absatz 1 sowie über die erteilten Genehmigungen nach Absatz 5.

(7) Sonstige datenschutzrechtliche Regelungen zur Übermittlung bleiben unberührt.

§ 9

Allgemeine Grundsätze: Zweckbindung, Erforderlichkeit, Datenvermeidung, Datensicherheit, Transparenz

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn es zur Erfüllung der Aufgaben oder der Geschäftszwecke der verarbeitenden Stelle erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben oder gespeichert worden sind. Dies gilt nicht für nicht automatisierte Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden. Die Zweckbegrenzung erfolgt grundsätzlich auch durch das genutzte Datenverarbeitungssystem und den jeweiligen Verarbeitungszusammenhang.

(2) Die Verarbeitung für einen anderen Zweck ist immer unzulässig, wenn dieser mit dem bisherigen Verarbeitungszweck unvereinbar ist. Die Erstellung von Persönlichkeitsprofilen ist unzulässig.

(3) Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um

1. so wenige personenbezogene Daten wie möglich zu verarbeiten,
2. die Ausführung datenschutzrechtlicher Vorschriften, insbesondere die Maßnahmen der Datensicherheit, sicherzustellen und
3. für die betroffenen Personen und für die Datenschutzkontrolle Öffentlichkeit und Nachvollziehbarkeit (Transparenz) zu gewährleisten.

§ 10

Besondere Regelungen zur Zweckbindung

(1) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes eines automatisierten Verfahrens oder Datenverarbeitungssystems gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(2) Eine Verarbeitung für andere Zwecke liegt nicht vor, soweit sie zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen oder der Rechnungsprüfung erforderlich ist. Dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken oder für die Durchführung von Organisationsuntersuchungen, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

§ 11

Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das

Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

§ 12

Verarbeitung besonderer Kategorien von Daten

(1) Die Verarbeitung von personenbezogenen Daten über ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit sowie über Gesundheit und Sexualleben sowie von Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet werden, für den sie sie erhalten hat, es sei denn, daß die Änderung des Zwecks durch eine Rechtsvorschrift zugelassen ist, die angemessene Garantien zum Schutz der in § 1 Abs. 1 genannten Grundrechte vorsieht.

(2) Für einen anderen Zweck dürfen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle zur Verfügung gestellt worden sind, nur verarbeitet werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

(3) Die Absätze 1 und 2 sind nicht anwendbar, wenn

1. die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich ist,
2. die betroffene Person aus tatsächlichen oder rechtlichen Gründen nicht in der Lage ist, ihre Einwilligung zu erteilen,
3. die Verarbeitung sich auf Daten bezieht, die die betroffene Person selbst öffentlich gemacht hat.

§ 13

Automatisierte Entscheidungen

Niemand darf einer Entscheidung mit rechtlichen Folgen oder erheblichen tatsächlichen Auswirkungen unterworfen werden, die ausschließlich auf die automatisierte Verarbeitung personenbezogener Daten gestützt wird, ohne daß der betroffenen Person die Geltendmachung der eigenen Interessen möglich gemacht worden ist.

ZWEITER UNTERABSCHNITT

Technische und organisatorische Maßnahmen

§ 14

Standardmaßnahmen

Bei der Verarbeitung personenbezogener Daten sind die Maßnahmen zu treffen, die nach Art der Verarbeitung gemäß dem Stand der Technik geeignet und angemessen sind,

1. Unbefugten den Zugang zu personenbezogenen Daten zu verwehren (Zugangskontrolle),
2. zu verhindern, daß gespeicherte Daten unbefugt genutzt, verändert oder gelöscht werden können (Datenträger-, Speicher- und Benutzerkontrolle),
3. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt werden können und übermittelt wurden (Übermittlungskontrolle),
4. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten wann von wem eingegeben, verändert, genutzt oder gelöscht worden sind (Eingabekontrolle),
5. zu gewährleisten, daß in einem vernetzten System überprüft und festgestellt werden kann, von welchen Systemteilen aus Daten genutzt, verändert oder weitergegeben worden sind (Netzkontrolle),
6. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können und verarbeitet werden (Auftragskontrolle),
7. zu verhindern, daß bei der Übertragung sowie beim Transport personenbezogene Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Übertragungs- und Transportkontrolle),
8. zu gewährleisten, daß personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
9. durch Dokumentation aller relevanten Verarbeitungsschritte die Revisionsfähigkeit eines Datenverarbeitungssystems sicherzustellen (Revisionskontrolle),
10. die Organisation der Stelle so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

§ 15

Besondere Maßnahmen

(1) Zur Verbesserung der Datensicherheit soll, soweit dies angemessen ist, eine Verschlüsselung von personenbezogenen Daten erfolgen. Sensible Daten sollen nur in verschlüsselter Form gespeichert und übermittelt werden.

(2) Die Verarbeitung personenbezogener Daten auf Systemen, zu denen der räumliche Zugang nicht besonderen Schutzvorkehrungen unterliegt, ist nur zulässig, wenn der unbefugte Zugriff hierauf durch geeignete Maßnahmen verhindert wird. Das gleiche gilt für Systeme, die elektronisch mit öffentlichen Netzen verbunden sind.

§ 16

Grundsätze der Systemgestaltung

(1) Die Erbringung einer Leistung darf nicht von einer Einwilligung der betroffenen Person in eine Verarbeitung ihrer Daten für andere Zwecke abhängig gemacht werden. Die Stelle hat die Leistung auch anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich ist. Die das Angebot in Anspruch nehmende Person ist über diese Möglichkeit zu informieren.

(2) Bei der Gestaltung und Auswahl informationstechnischer Produkte hat die verarbeitende Stelle sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten. Sie hat zu prüfen, ob deren Einsatz mit den Regelungen des Datenschutzrechts vereinbar ist. Produkte, deren Vereinbarkeit mit den Regeln des Datenschutzes und der Datensicherheit in einem förmlichen Verfahren geprüft und positiv bewertet worden sind, sollen vorrangig berücksichtigt werden.

§ 17

Datenschutz-Audit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 18

Behördlicher bzw. betrieblicher Datenschutzbeauftragter

(1) Stellen, die personenbezogene Daten automatisiert verarbeiten und hierbei in der Regel mindestens fünf Bedienstete ständig beschäftigen, haben unter Beteiligung der Vertretung der Beschäftigten in entsprechender Anwendung von § 99 des Betriebsverfassungsgesetzes einen Datenschutzbeauftragten zu bestellen. Dieser muß die erforderliche persönliche und fachliche Qualifikation und Eignung besitzen. Werden in der Regel mindestens 500 Bedienstete bei der automatisierten Datenverarbeitung eingesetzt, so ist ein Bediensteter für die Wahrnehmung der Aufgaben des Datenschutzbeauftragten vollständig freizustellen.

(2) Der Datenschutzbeauftragte unterstützt die Stelle bei der Sicherstellung des Datenschutzes. Er hat insbesondere

1. die Einhaltung sowie die Umsetzung der datenschutzrechtlichen Vorschriften zu überprüfen,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen über die jeweils spezifischen Erfordernisse für den Datenschutz zu unterrichten,
3. bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen und bei der Auswahl der Verarbeitungssysteme und -programme beratend mitzuwirken,
4. bei der Einführung oder der wesentlichen Änderung von automatisierten Verfahren, bei denen keine Technikfolgenabschätzung nach § 20 erfolgt, eine entsprechende Vorabkontrolle durchzuführen.

(3) Der Datenschutzbeauftragte ist dem Leiter oder dem Leitungsorgan der verarbeitenden Stelle unmittelbar zu unterstellen. Er ist bei der Anwendung der Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Seine Bestellung darf nur widerrufen werden auf Verlangen der zuständigen Datenschutzkontrollinstanz oder, nach Beteiligung der Vertretung der Beschäftigten in entsprechender Anwendung von § 99 des Betriebsverfassungsgesetzes, wenn dies wegen mangelhafter Ausübung der Aufgaben oder aus organisatorischen Gründe der verarbeitenden Stelle zwingend erforderlich ist. Er kann sich jederzeit an die zuständige Datenschutzkontrollinstanz wenden.

(4) Die verarbeitende Stelle hat den Datenschutzbeauftragten bei der Ausführung seiner Aufgaben zu unterstützen. Er ist über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten. Er ist zur Wahrnehmung seiner Aufgaben freizustellen und angemessen mit personellen und sächlichen Mitteln auszustatten. Bedienstete sowie die Vertretung der Beschäftigten können sich jederzeit an den Datenschutzbeauftragten wenden.

(5) Dem Datenschutzbeauftragten ist von der verarbeitenden Stelle eine Übersicht zur Verfügung zu stellen über die in § 19 Abs. 2 genannten Angaben. Er hat diese Angaben jeder beantragenden Person in geeigneter Weise verfügbar zu machen.

(6) Der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf diese zulassen, verpflichtet, soweit er von der betroffenen Person davon nicht befreit wurde.

§ 19

Meldepflicht

(1) Stellen,

1. deren Verarbeitung personenbezogener Daten wegen der Art der Daten, der Verarbeitung und der voraussichtlichen Empfänger eine besondere Gefahr für den Schutz der in § 1 Abs. 1 genannten Grundrechte besteht und die keinen Datenschutzbeauftragten bestellt haben,
2. die personenbezogene Daten zum Zweck der Übermittlung oder im Auftrag als Dienstleistungsunternehmen verarbeiten, es sei denn, dies stellt wegen der Geringfügigkeit der Verarbeitung keine wesentliche Gefahr für den Schutz der in § 1 Abs. 1 genannten Grundrechte dar,

haben vor Aufnahme, Veränderung und Beendigung ihrer Tätigkeit dies der zuständigen Datenschutzkontrollinstanz mitzuteilen.

(2) Bei der Anmeldung sind folgende Angaben zu machen:

1. Name oder Firma und Anschrift der speichernden Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige rechtlich berufene Leiter und die mit der Leitung beauftragten Personen,
3. die Zwecke der Datenverarbeitung,
4. eine Beschreibung der Kategorien der betroffenen Personen und der verarbeiteten Daten,
5. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
6. soweit vorhanden, Name des Datenschutzbeauftragten,
7. Regelfristen für die Datenlöschung,
8. geplante Datenübermittlungen in Drittländer,
9. eine allgemeine Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen und der Datensicherungsmaßnahmen nach § 14.

(3) Die Datenschutzkontrollinstanzen führen ein Register mit den in Absatz 2 aufgeführten Angaben. Das Register kann von jeder Person eingesehen werden.

(4) Das Nähere, insbesondere unter welchen Umständen keine Meldepflicht besteht, wird durch Rechtsverordnung festgelegt.

§ 20

Vorabkontrolle durch Technikfolgenabschätzung

(1) Vor der Entscheidung über den Einsatz oder die wesentliche Änderung von automatisierten Verfahren, von denen spezifische Risiken für die in § 1 Abs. 1 genannten Grundrechte oder für die Wirkungsmöglichkeiten demokratischer Organe ausgehen können, ist eine Technikfolgenabschätzung durchzuführen. Die zuständige Datenschutzkontrollinstanz ist bei der Abschätzung zu beteiligen. Dies gilt auch für gemeinnützige Verbände, deren Zielsetzung in der Verwirklichung der in § 1 Abs. 1 genannten Grundrechte liegt und die auf Antrag vom zuständigen Bundesministerium hierzu zugelassen werden. Das Ergebnis der Technikfolgenabschätzung und seine Begründung werden von der verarbeitenden Stelle veröffentlicht. Die Verfahren dürfen nur eingesetzt oder wesentlich geändert werden, soweit durch technische oder organisatorische Maßnahmen sichergestellt wird, daß die spezifischen Risiken wirksam beherrscht werden können.

(2) Das Nähere wird durch Rechtsverordnung bestimmt.

DRITTER UNTERABSCHNITT

Betroffenenrechte

§ 21

Unabdingbarkeit

Die Rechte der betroffenen Person zu Auskunft, Anrufung der zuständigen Datenschutzkontrollinstanz und Datenkorrektur können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

§ 22

Sicherung der Betroffenenrechte

(1) Sind die Daten der betroffenen Person so gespeichert, daß mehrere Stellen verarbeitungsberechtigt sind, so kann sie sich an jede dieser Stellen zur Wahrnehmung ihrer Rechte wenden. Diese ist verpflichtet, das Vorbringen der betroffenen Person an die verarbeitende Stelle weiterzuleiten. Die betroffene Person ist über die Weiterleitung und die speichernde Stelle zu unterrichten.

(2) Erstrebt die betroffene Person eine Überprüfung der Datenverarbeitung auf Grund einer eigenen Initiative (Anrufung einer Datenschutzkontrollinstanz, Ersuchen auf Auskunft, Berichtigung, Sperrung, Schadensersatz), so ist eine Datenlöschung unzulässig.

§ 23

Auskunft an die betroffene Person

(1) Der betroffenen Person ist auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person verarbeiteten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen,
2. den Zweck der Verarbeitung,
3. die organisatorische Struktur und den logischen Aufbau der automatisierten Verarbeitung in bezug auf ihre Daten.

(2) Begehrt der Antrag Auskunft über nicht automatisiert gespeicherte Daten, so soll dieser Angaben enthalten, die das Auffinden der Daten ermöglichen. Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen bestimmter überwiegender Interessen von Dritten geheimgehalten werden müssen.

(4) Die vollständige oder teilweise Ablehnung der Auskunftserteilung ist zu begründen. Die betroffene

Person ist darauf hinzuweisen, daß sie sich an die zuständige Datenschutzkontrollinstanz wenden kann.

(5) Die Auskunft ist unentgeltlich.

(6) Das Verlangen, eine schriftliche Auskunft vor Abschluß eines Vertrages, der für die betroffene Person von besonderer Bedeutung ist, vorzulegen, ist unzulässig.

§ 24

Benachrichtigung

(1) Werden Daten nicht bei der betroffenen Person erhoben, so ist sie über die gepeicherten Daten, die speichernde Stelle, die Zweckbestimmung der Verarbeitung, die Empfänger oder Kategorien von Empfänger sowie das Bestehen von Auskunfts- und Datenkorrekturrechten zu unterrichten. Ist eine Übermittlung vorgesehen, so hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. die betroffene Person auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur wegen gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften oder zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes (§ 10 Abs. 1) gespeichert werden,
3. die Speicherung oder Übermittlung durch Gesetz zwingend vorgesehen ist,
4. die Speicherung oder Übermittlung Zwecken der Strafverfolgung, der Verfolgung von Ordnungswidrigkeiten oder der Gefahrenabwehr dient,
5. die Daten wegen eines überwiegenden rechtlichen Interesses eines Dritten oder wegen eines öffentlichen Interesses geheimgehalten werden müssen,
6. die Daten von der verarbeitenden Stelle nach § 45 automatisiert veröffentlicht werden dürfen oder
7. die Speicherung nach § 46 Abs. 4 der Markt- und Meinungsforschung dient.

(3) Hat die verarbeitende Stelle Grund zur Annahme oder Kenntnis davon, daß unrichtige oder unzulässig verarbeitete Daten bereits derart genutzt wurden, daß der betroffenen Person daraus ein Nachteil entstanden ist oder zu entstehen droht, so hat sie diese unverzüglich zu benachrichtigen.

§ 25

Datenkorrektur (Berichtigung, Löschung und Sperrung)

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. ihre Kenntnis für die speichernde Stelle zur Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist oder
3. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung am Ende des dritten Kalenderjahres nach der erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden oder
3. bei einer nicht öffentlichen Stelle die Richtigkeit der personenbezogenen Daten bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(4) Sind zu korrigierende personenbezogene Daten nicht automatisiert gespeichert und ist eine Datenkorrektur aus tatsächlichen oder rechtlichen Gründen nicht möglich, so ist dies in den Unterlagen, z.B. durch Hinzufügen einer Gegendarstellung, zu vermerken. Erfolgt eine weitere Verarbeitung, so sind diese Vermerke zu berücksichtigen.

(5) Von der Berichtigung, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen unzulässiger Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben werden, es sei denn, dies ist zur Wahrung der schutzwürdigen Interessen der betroffenen Person nicht erforderlich.

(6) Gesperrte Daten dürfen ohne Einwilligung der betroffenen Person nur verarbeitet werden, wenn

1. dies zur Behebung einer Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist,
2. für wissenschaftliche Zwecke, wenn diese gegenüber den Interessen der betroffenen Person erheblich überwiegen

und die Daten hierfür verarbeitet werden dürften, wenn sie nicht gesperrt wären.

§ 26

Recht auf Datensicherung

Die betroffene Person hat das Recht, die Maßnahmen zur Sicherung von Vertraulichkeit und Unverletzlichkeit zu ergreifen, die sie für erforderlich hält.

§ 27

Anrufung der Datenschutzkontrollinstanz

(1) Jede Person kann sich direkt an eine Datenschutzkontrollinstanz wenden, wenn sie der Ansicht

ist, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein. Dies gilt auch für Beschäftigte der verarbeitenden Stelle. Keine Person darf deswegen benachteiligt werden.

(2) Ist die angerufene Stelle nicht zuständig, so gibt sie die Eingabe an die zuständige Stelle ab. Die Person wird informiert, wie mit ihrer Eingabe verfahren wurde.

§ 28

Widerspruchsrecht

Die betroffene Person hat das Recht, aus besonderen persönlichen Gründen gegenüber der verarbeitenden Stelle der Verarbeitung ihrer Daten allgemein oder bestimmter Formen der Verarbeitung zu widersprechen. Sie ist über das Ergebnis der Prüfung ihres Widerspruchs zu unterrichten. Ergibt die Prüfung, daß einer Datenverarbeitung schutzwürdige Interessen der betroffenen Person entgegenstehen, so ist die Verarbeitung unzulässig.

§ 29

Schadensersatz

(1) Entsteht der betroffenen Person durch eine datenschutzrechtlich unzulässige oder unrichtige Verarbeitung ihrer personenbezogenen Daten ein Schaden, so ist die verarbeitende Stelle oder deren Träger unabhängig von einem Verschulden zum Ersatz des daraus entstandenen Schadens verpflichtet. Bei Verletzung des Persönlichkeitsrechts ist ein Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(2) Ist streitig, ob ein Schaden ursächliche Folge einer unzulässigen oder unrichtigen Verarbeitung ist, so trifft die Beweislast die speichernde Stelle. Sind mehrere Stellen verarbeitende Stellen und ist die geschädigte Person nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen. Mehrere Ersatzpflichtige haften als Gesamtschuldner. Auf das Mitverschulden der betroffenen Person und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden. Solange eine Überprüfung durch die zuständige Datenschutzkontrollinstanz erfolgt, ist die Verjährungsfrist gehemmt. Weitergehende Schadensersatzansprüche bleiben unberührt.

(3) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

VIERTER UNTERABSCHNITT

Besondere Formen der Datenverarbeitung

§ 30

Einsatz automatisierter Abruf- und Verbundverfahren

(1) Der Einsatz eines

1. automatisierten Verfahrens, das die Übermittlung personenbezogener Daten, die in dieser Form nicht aus allgemein zugänglichen Quellen entnommen werden können, durch Abruf ermöglicht,
2. Verbundverfahrens, bei dem verschiedene Stellen personenbezogene Daten in einem gemeinsamen Datenbestand verarbeiten,

ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der betroffenen Person und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Beteiligung von öffentlichen und nicht öffentlichen Stellen an einem Verfahren ist unzulässig.

(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Verfahrens nach Absatz 1 kontrolliert werden kann. Sie haben schriftlich festzulegen:

1. Anlaß und Zweck des Verfahrens,
2. eine Stelle, gegenüber der Betroffenenrechte insgesamt geltend gemacht werden können,
3. verarbeitende Stellen und Empfänger,
4. Art der zu übermittelnden Daten und
5. nach § 14 erforderliche technische und organisatorische Maßnahmen.

(3) Über den Einsatz von Verfahren nach Absatz 1 sind die für die beteiligten Stellen zuständigen Datenschutzkontrollinstanzen unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. Die speichernde Stelle protokolliert die einzelnen Abrufe. Sie prüft die Zulässigkeit der Abrufe, wenn dazu Anlaß besteht. Die speichernde Stelle hat zu gewährleisten, daß die Zulässigkeit der Übermittlung zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann und überprüft wird.

§ 31

Datenverarbeitung im Auftrag, externe Wartung

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet, ist der Auftraggeber für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Betroffenenrechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ergeben sich für ihn Hinweise, daß bei der Verarbeitung gegen datenschutzrechtliche Vorschriften verstoßen wird, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten nur die §§ 11, 14, 15, 18, 19, 54 und 55 sowie die Vorschriften über die Datenschutzkontrolle.

(5) Personen und Stellen, die mit der Wartung und Systembetreuung automatisierter Verfahren oder Datenverarbeitungssysteme beauftragt sind, unterliegen den Absätzen 1 bis 4. Sie müssen die notwendige fachliche Qualifikation und Zuverlässigkeit aufweisen. Die Dokumentation der Maßnahmen ist zum Zweck der Datenschutzkontrolle drei Jahre aufzubewahren. Soweit erforderlich, ist eine Kenntnisnahme von Berufs- und besonderen Amtsgeheimnissen sowie von sensiblen Daten zulässig.

§ 32

Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien

(1) Der Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien, die von den betroffenen Personen mit sich geführt werden und die mit elektronischen Lese- und Schreibgeräten direkt kommunizieren, ist nur zulässig, soweit ein Gesetz dies vorsieht oder die betroffene Person eingewilligt hat. Verarbeitende Stelle ist diejenige, die Kontrolle über das Verfahren oder über den jeweiligen Verfahrensteil hat.

(2) Jede Kommunikation zwischen mobilen Speicher- und Verarbeitungsmedien und elektronischen Lese- und Schreibgeräten muß für die betroffene Person erkennbar sein. Erfolgt bei dieser Kommunikation eine Datenspeicherung, so ist sicherzustellen, daß die betroffene Person hierüber einen schriftlichen Nachweis erhalten kann.

(3) Der Anspruch auf Auskunft über alle auf einem Speicher- und Verarbeitungsmedium zu ihrer Person gespeicherten Daten ist durch angemessene Bereitstellung von Endgeräten durch die speichernden Stellen sicherzustellen. Soweit nicht ein Gesetz anderes vorsieht, darf niemand gezwungen werden, mobile Speicher- und Verarbeitungsmedien oder Ausdrucke ihres Inhalts vorzulegen.

(4) Werden mobile Speicher- und Verarbeitungsmedien mit Einwilligung der betroffenen Person eingesetzt, so ist diese vor der Erteilung der Einwilligung zu unterrichten über

1. die zur Speicherung und zum Abruf berechtigten Stellen,
2. die Organisation der Zugriffs- und Speicherungsbeschränkung sowie
3. die Möglichkeit des vollständigen oder teilweisen Widerrufs der Einwilligung.

Die Ausgabe und Verwendung von mobilen Speicher- und Verarbeitungsmedien darf für die betroffene Person nicht mit Vergünstigungen verbunden sein, die über das durch die Technik bedingte Maß hinausgehen.

§ 33

Videoüberwachung

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, soweit dies zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, daß schutzwürdige Interessen der betroffenen Personen überwiegen. Der Umstand der Beobachtung ist durch geeignete Maßnahmen erkennbar zu machen.

(2) Die Speicherung von nach Absatz 1 Satz 1 erhobenen Daten ist zulässig, wenn dies zum Erreichen des verfolgten Zweckes dringend erforderlich ist. Die Daten sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind.

(3) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet und verarbeitet, so ist diese zu benachrichtigen, es sei denn, dem stehen überwiegende öffentliche Interessen der Strafverfolgung oder der Gefahrenabwehr entgegen.

ZWEITER ABSCHNITT

Datenverarbeitung der öffentlichen Stellen

§ 34

Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Für Landesbeauftragte für den Datenschutz gilt § 38 Abs. 6 entsprechend.

ERSTER UNTERABSCHNITT

Voraussetzungen für die Zulässigkeit

§ 35

Zulässigkeit der Verarbeitung

Die Verarbeitung personenbezogener Daten ist zur Erfüllung der Aufgaben der verarbeitenden Stelle zulässig, wenn

1. die betroffene Person eingewilligt hat,
2. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
3. dies zur Abwehr von Gefahren für Leib, Leben oder die persönliche Freiheit erforderlich ist,
4. Angaben der betroffenen Person überprüft werden müssen, weil Anhaltspunkte für deren Unrichtigkeit bestehen,
5. offensichtlich ist, daß die Verarbeitung im Interesse der betroffenen Person liegt und sie einwilligen würde,

6. die Daten aus allgemein zugänglichen Quellen entnommen werden können,
7. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten ist.

§ 36

Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist nur zulässig, wenn die Übermittlung zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Daten nach § 35 verarbeitet werden dürfen.

(2) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist deren Übermittlung auch zulässig, soweit nicht berechtigte Interessen der betroffenen Person an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig; der Empfänger ist hierauf hinzuweisen.

(3) Die Absätze 1 und 2 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 37

Übermittlung an Empfänger außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 35 verarbeitet werden dürfen,
2. der Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse der betroffenen Person an der Geheimhaltung überwiegt oder
3. sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die betroffene Person, nachdem sie über die beabsichtigte Übermittlung in geeigneter Weise und rechtzeitig unterrichtet worden ist, nicht widersprochen hat.

(2) Der Empfänger darf die übermittelten Daten nur für den Zweck nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

ZWEITER UNTERABSCHNITT

Bundesbeauftragter für den Datenschutz

§ 38

Rechtsstellung

(1) Der Bundesbeauftragte für den Datenschutz wird als oberste Bundesbehörde eingerichtet. Er ist in der Ausübung des Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienst- und Rechtsaufsicht der Bundesregierung.

(2) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten. Der Gewählte ist vom Bundespräsidenten zu ernennen. Ist der Bundesbeauftragte vorübergehend an der Ausübung seiner Amtes verhindert, kann die Bundesregierung einen Vertreter mit der Wahrnehmung der Geschäfte beauftragten, nachdem dem Bundesbeauftragten Gelegenheit zur Stellungnahme gegeben wurde.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen.

(5) Der Bundesbeauftragte darf neben seinem Amt kein besoldetes Amt, kein Gewerbe und keinen Beruf und keine vergleichbare Tätigkeit ausüben. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(6) Der Bundesbeauftragte ist berechtigt, über Personen und Tatsachen, die ihm in seiner amtlichen Eigenschaft anvertraut worden sind, das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeitenden des Bundesbeauftragten mit der Maßgabe, daß dieser über die Ausübung dieses Rechts entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf das Vorlegen oder die Auslieferung von Akten oder anderen Unterlagen von ihm nicht gefordert werden.

(7) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Er darf, auch wenn er nicht mehr im Amt ist, ohne Genehmigung der Bundesregierung weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen. Die Genehmigung soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde.

§ 39

Kontrolle durch den Bundesbeauftragten

(1) Der Bundesbeauftragte kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der da-

tenschutzrechtlichen Vorschriften. Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(2) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, Daten und Datenverarbeitungsprogramme zu gewähren,
2. jederzeit Zutritt in alle Diensträume und Zugriff zu elektronischen Diensten zu gewähren,
3. Kopien von Unterlagen, von automatisiert gespeicherten Daten und Verarbeitungsprogrammen zur Verfügung zu stellen.

(3) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Beiseitigung festgestellter Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

§ 40

Beanstandungen durch den Bundesbeauftragten

(1) Stellt der Bundesbeauftragte Verstöße gegen datenschutzrechtliche Vorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, bei deren Vereinigungen sowie bei sonstigen öffentlichen Stellen des Bundes gegenüber dem Vorstand, dem sonst vertretungsberechtigten Organ oder dem Leiter

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. Besteht eine Aufsichtsbehörde, so wird diese über die Beanstandung unterrichtet.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung getroffen worden sind.

§ 41

Weitere Aufgaben und Befugnisse des Bundesbeauftragten

(1) Der Bundesbeauftragte erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im nicht öffentlichen Bereich enthalten.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Er geht Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Er kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte berät Stellen und Organe des Bundes in allen Angelegenheiten des Datenschutzes. Er ist rechtzeitig über Planungen zum Aufbau bedeutender Datenverarbeitungssysteme und über geplante Rechts- und Verwaltungsvorschriften, die das Recht auf informationelle Selbstbestimmung betreffen, zu unterrichten.

(4) Die Übermittlung personenbezogener Daten durch den Bundesbeauftragten an Datenschutzkontrollinstanzen sowie an entsprechende Einrichtungen der Länder und der Mitgliedstaaten der Europäischen Union ist zulässig, soweit dies zur Aufgabenerfüllung des Bundesbeauftragten oder des Empfängers erforderlich ist. § 10 Abs. 1 gilt entsprechend; der Empfänger ist hierauf hinzuweisen.

(5) Der Bundesbeauftragte nimmt weitere Aufgaben wahr, soweit diese ihm durch Gesetz übertragen werden.

DRITTER ABSCHNITT

Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

§ 42

Anwendungsbereich

Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten verarbeitet werden durch

1. nicht öffentliche Stellen gemäß § 1 Abs. 2 Nr. 2,
2. öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

In den Fällen der Nummer 2 gelten anstelle des § 48 die §§ 39 bis 41.

§ 43

Datenverarbeitung für eigene Zwecke

(1) Die Verarbeitung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit der betroffenen Person,
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle, berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist und kein Grund zur Annahme besteht, daß das

schutzwürdige Interesse der betroffenen Person am Ausschluß der Verarbeitung überwiegt,

3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verarbeitende Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse der betroffenen Person an dem Ausschluß der Verarbeitung offensichtlich überwiegt.

(2) Der Dritte, dem personenbezogene Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung ist auch zulässig, wenn dem Dritten die Daten für den anderen Zweck hätten übermittelt werden dürfen und die übermittelnde Stelle der Nutzung zustimmt. Die übermittelnde Stelle hat den Dritten auf die Zweckbindung hinzuweisen.

§ 44

Geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung

(1) Das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß die betroffene Person ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse der betroffenen Person an dem Ausschluß der Speicherung und Veränderung offensichtlich überwiegt.

(2) Die Übermittlung ist zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, daß die betroffene Person ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung sind von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Empfänger. Für die Verarbeitung der übermittelten Daten gilt § 43 Abs. 2 entsprechend.

§ 45

Automatisierte Veröffentlichung

(1) Das automatisierte Veröffentlichen personenbezogener Daten ist nur zulässig, soweit die betroffene Person eingewilligt hat. Eine Übernahme personenbezogener Daten von Druckwerken zum Zweck der automatisierten Veröffentlichung ist nur zulässig, soweit eine entsprechende Einwilligung in dem Druckwerk besonders vermerkt ist.

(2) Das automatisierte Veröffentlichen ist unzulässig, soweit die betroffene Person dem durch kostenfreie Eintragung in einer Widerspruchsliste beim Bundesbeauftragten für den Datenschutz widersprochen hat. Der Bundesbeauftragte stellt diese Liste gegen eine angemessene Gebühr auf Anfrage zur Verfügung. Die Widersprüche sind innerhalb von vier Wochen zu berücksichtigen. Eine Nutzung dieser Daten für andere Zwecke ist unzulässig. Erfolgt die Veröffentlichung zu einem festen Datum, so ist dieses in oder auf der Veröffentlichung zu vermerken.

(3) Vor der erstmaligen Veröffentlichung ist der Bundesbeauftragte für den Datenschutz unter Angabe der veröffentlichten Daten zu unterrichten. Dieser führt hierüber ein Register. Das Register kann von jeder Person eingesehen und genutzt werden.

(4) Hat die betroffene Person der automatisierten Veröffentlichung ihrer personenbezogenen Daten in elektronischen Verzeichnissen gegenüber der verarbeitenden Stelle widersprochen, so ist diese unzulässig.

§ 46

Datenverarbeitung zum Zweck der Werbung und der Markt- und Meinungsforschung

(1) Die Verarbeitung für Zwecke der Werbung oder der Markt- oder Meinungsforschung ist unzulässig, wenn die betroffene Person

1. gegenüber der verarbeitenden Stelle widersprochen hat oder
2. sich beim Bundesbeauftragten für den Datenschutz in die Werbestoppliste eintragen ließ und zuvor kein Kundenkontakt bestanden hat.

(2) Natürliche Personen können sich beim Bundesbeauftragten für den Datenschutz kostenfrei in eine Werbestoppliste eintragen lassen. Der Bundesbeauftragte stellt diese Liste gegen eine angemessene Gebühr auf Anfrage zur Verfügung. Vier Wochen oder weniger vor einer Maßnahme nach Absatz 1 muß ein Abgleich mit der Liste vorgenommen werden, wenn zuvor kein Kundenkontakt bestanden hat. Eine Nutzung dieser Daten für andere Zwecke ist unzulässig.

(3) Die betroffene Person ist bei der Ansprache zum Zweck der Werbung oder der Markt- und Meinungsforschung über die speichernde Stelle, über die Herkunft der Daten, über die Kriterien der Auswahl sowie über das Widerspruchsrecht nach Absatz 1 zu unterrichten.

(4) Werden personenbezogene Daten zum Zweck der Übermittlung in anonymisierter Form für die Markt- und Meinungsforschung gespeichert, sind die Merkmale gesondert zu speichern, mit denen Angaben über persönliche oder sachliche Verhältnisse einer natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Angaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

§ 47

Verarbeitung besonderer Kategorien von Daten

Bei der Verarbeitung besonderer Kategorien von Daten gemäß § 12 Abs. 1 ist, unbeschadet von § 12,

grundsätzlich davon auszugehen, daß Grund zu der Annahme besteht, daß die betroffene Person ein schutzwürdiges Interesse an dem Ausschluß der Verarbeitung hat. Dies gilt auch für Daten, die sich auf strafbare Handlungen, auf Ordnungswidrigkeiten sowie auf arbeitsrechtliche Verhältnisse beziehen.

§ 48

Aufsichtsbehörde

(1) Die Aufsichtsbehörde überprüft die Ausführung datenschutzrechtlicher Vorschriften.

(2) Die überprüften Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde zur Erfüllung ihrer Aufgaben auf Verlangen

1. die erforderlichen Auskünfte unverzüglich zu erteilen,
2. geschäftliche Unterlagen, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen, vorzulegen,
3. Kopien von automatisiert verarbeiteten Daten und Verarbeitungsprogrammen zur Verfügung zu stellen,
4. während der Betriebs- und Geschäftszeiten Zutritt zu Grundstücken und Geschäftsräumen zu gewähren,
5. Zugang zu Verfahren automatisierter Datenverarbeitung zu gewähren.

(3) Die Auskunft nach Absatz 2 Nr. 1 kann auf solche Fragen verweigert werden, deren Beantwortung den Auskunftspflichtigen selbst oder einen der in § 383 Abs. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Zur Gewährleistung des Datenschutzes kann die Aufsichtsbehörde

1. anordnen, daß im Rahmen der Anforderungen nach den §§ 14 bis 16 und 18 bis 20 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden,
2. feststellen, daß bestimmte Formen der Verarbeitung personenbezogener Daten unzulässig sind.

Bei schwerwiegenden Mängeln kann sie den Einsatz einzelner Verfahren untersagen, wenn Mängel entgegen einer Anordnung bzw. Feststellung nach Satz 1 in angemessener Zeit nicht beseitigt wurden. Sie kann die Abberufung des Datenschutzbeauftragten verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(5) Die Aufsichtsbehörde führt das Register nach § 19 Abs. 3. § 41 Abs. 4 gilt entsprechend. Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen unabhängigen Aufsichtsbehörden.

(6) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

VIERTER ABSCHNITT

Sondervorschriften

§ 49

Verhaltensregeln

(1) Berufsverbände, andere Vereinigungen, die bestimmte Gruppen von verarbeitenden Stellen vertreten, sowie Vereinigungen, deren Zielsetzung im Schutz der in Artikel 1 Abs. 1 genannten Grundrechte liegt, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Vorschriften der zuständigen Datenschutzkontrollinstanz unterbreiten.

(2) Die zuständige Datenschutzkontrollinstanz stellt die Vereinbarkeit der ihr vorgelegten Entwürfe mit dem geltenden Recht fest und veröffentlicht diese.

§ 50

Datenverarbeitung bei Beschäftigungsverhältnissen

(1) Die Verarbeitung personenbezogener Daten über frühere, bestehende oder zukünftige Beschäftigungsverhältnisse ist zulässig, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag, eine Betriebs- oder eine Dienstvereinbarung dies vorsieht.

(2) Für öffentliche Stellen des Bundes gelten die §§ 90 bis 90g des Bundesbeamtengesetzes in der jeweils geltenden Fassung gegenüber den in Absatz 1 genannten Personen, die hiervon nicht erfaßt werden, entsprechend.

(3) Bei der erstmaligen automatisierten Speicherung ist der betroffenen Person die Art der über sie gespeicherten Daten mitzuteilen; bei wesentlichen Änderungen ist sie zu benachrichtigen.

(4) Eine Übermittlung ist nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt oder die Art und Zielsetzung der dem Beschäftigten übertragenen Aufgaben dies erfordern. Die Übermittlung an künftige Arbeitgeber ist nur mit Einwilligung der betroffenen Person zulässig.

(5) Die Weiterverarbeitung der bei ärztlichen oder psychologischen Untersuchungen und Tests zum Zweck der Eingehung eines Beschäftigungsverhältnisses erhobenen Daten ist nur mit Einwilligung der betroffenen Person zulässig. Der Arbeitgeber darf von der untersuchenden Person oder Stelle grund-

sätzlich nur das Ergebnis der Eignungsuntersuchung und die dabei festgestellten Risikofaktoren anfordern. Fordert der Arbeitgeber weitere personenbezogene Daten an, so hat er die Gründe hierfür aufzuzeichnen. Die betroffene Person ist zuvor zu unterrichten. Personenbezogene Daten, die zur Aufzeichnung des Bewerbungsvorgangs nicht erforderlich sind, sind unverzüglich zu löschen, sobald feststeht, daß ein Beschäftigungsverhältnis nicht zustande kommt. Dies gilt nicht, wenn die betroffene Person in die weitere Speicherung schriftlich eingewilligt hat.

(6) Medizinische und psychologische Befunde von Beschäftigten dürfen von personalverwaltenden Stellen nicht in automatisierten Verfahren verarbeitet werden. Dies gilt nicht für Daten, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden.

§ 51

Datenverarbeitung zum Zweck wissenschaftlicher Forschung

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.

(2) Die Verarbeitung für Zwecke der wissenschaftlichen Forschung ist zulässig, wenn

1. die betroffene Person hierin eingewilligt hat,
2. schutzwürdige Interessen der betroffenen Person wegen der Art der Daten oder wegen der Art der Verarbeitung für das jeweilige Forschungsvorhaben nicht beeinträchtigt werden oder
3. nach schriftlicher Feststellung des Datenschutzbeauftragten das öffentliche Interesse an dem jeweiligen Forschungsvorhaben gegenüber dem schutzwürdigen Interesse der betroffenen Person überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Der Datenschutzbeauftragte hat der zuständigen Datenschutzkontrollinstanz einmal jährlich eine Aufstellung aller nach Nummer 3 durchgeführten Forschungsvorhaben mitzuteilen.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale, mit deren Hilfe ein Bezug auf eine bestimmte natürliche Person hergestellt werden kann, gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck dies gestattet.

(4) Die wissenschaftliche Forschung betreibende Stelle darf personenbezogene Daten nur veröffentlichen, wenn

1. die betroffene Person eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte erforderlich ist.

(5) Die übermittelnde Stelle hat Empfänger, auf die dieses Gesetz keine Anwendung findet, zu verpflichten, die Vorschriften der Absätze 1, 3 und 4 einzuhalten.

§ 52

Datenverarbeitung durch die Medien

(1) Soweit personenbezogene Daten von Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films (Medienunternehmen) ausschließlich zu eigenen journalistischen-redaktionellen, künstlerischen oder literarischen Zwecken verarbeitet werden, gelten von den Vorschriften dieses Gesetzes nur die §§ 11 (Datengeheimnis), 14 bis 17 (technisch-organisatorische Maßnahmen) und 28 (Widerspruchsrecht). An die Stelle der Datenschutzkontrollinstanz tritt insoweit der Medien-Datenschutzbeauftragte, auf den § 18, ausgenommen Absatz 3 Satz 3 erste Alternative und Satz 4, sowie § 27 anzuwenden sind.

(2) Führt die Verarbeitung nach Absatz 1 zur Veröffentlichung von Gegendarstellungen der betroffenen Person, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Rundfunkanstalten des Bundesrechts in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder der Gewährsperson von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Die betroffene Person kann die Berichtigung unrichtiger Daten oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen.

(4) Die geschäftsmäßige automatisierte Veröffentlichung von personenbezogenen Daten aus Medienarchiven, die erstmals vor mehr als fünf Jahren veröffentlicht worden sind, ist unzulässig. Die Übermittlung dieser Daten ist zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. § 44 Abs. 2 gilt entsprechend.

FÜNFTER ABSCHNITT

Schlußvorschriften

§ 53

Unterrichtung der Staatsanwaltschaft

Erhält die Datenschutzkontrollinstanz im Rahmen der Wahrnehmung ihrer Aufgaben Kenntnis von möglicherweise strafbaren Sachverhalten, so kann sie hierüber die zuständige Staatsanwaltschaft unterrichten.

§ 54

Strafvorschriften

(1) Wer gegen Entgelt oder in der Absicht, sich oder eine andere Person zu bereichern oder eine andere Person zu schädigen, unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. speichert, verändert oder übermittelt,
2. zum Abruf mittels automatisierten Verfahrens bereithält oder
3. abruft oder sich oder einem anderen beschafft,
4. dadurch erzeugt, daß er anonymisierte Daten mit anderen Informationen zusammenführt und dadurch die betroffene Person bestimmbar macht,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 55

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. personenbezogene Daten, die nicht offenkundig sind, entgegen § 11 zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeitet oder offenbart,
2. sich durch Vortäuschung falscher Tatsachen personenbezogene Daten, die nicht offenkundig sind, verschafft oder an sich oder andere übermitteln läßt,
3. entgegen § 18 Abs. 1 einen Datenschutzbeauftragten nicht oder nicht rechtzeitig bestellt,
4. entgegen § 19 Abs. 1 eine Meldung nicht, nicht rechtzeitig oder entgegen § 19 Abs. 2 nicht richtig oder nicht vollständig erstattet,
5. entgegen § 23 Abs. 3 vor Vertragsabschluß die Vorlage einer Auskunft verlangt,
6. entgegen § 24 Abs. 1 die betroffene Person nicht, nicht richtig oder nicht vollständig benachrichtigt,
7. entgegen § 44 Abs. 2 oder § 52 Abs. 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
8. entgegen § 48 Abs. 2 Nr. 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,
9. den in § 48 Abs. 2 Nr. 2 bis 5 genannten Pflichten nicht nachkommt,
10. oder der Beseitigungsanordnung festgestellter Mängel nach § 48 Abs. 4 Satz 2 nicht nachkommt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu einhunderttausend Deutsche Mark geahndet werden.

§ 56

Übergangsvorschrift

Solange bereichsspezifische Regelungen des Bundes nicht an die Begriffsbestimmungen des § 3 Abs. 3 angepaßt wurden, gilt § 3 Abs. 4 bis 6 des Bundesdatenschutzgesetzes (BDSG) 1990 fort.

§ 57

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft.

(2) Mit dem Inkrafttreten dieses Gesetzes tritt das Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch ..., außer Kraft.

Bonn, den 28. Oktober 1997

Manfred Such
Joseph Fischer (Frankfurt), Kerstin Müller (Köln) und Fraktion

Begründung

Allgemeines

Erste Zielsetzung: Anpassung an die EU-Datenschutzrichtlinie

Am 24. Oktober 1995 trat die „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (EU-DSRL) in Kraft (ABl. EG Nr. L 281 S. 31 vom 23. November 1995). Diese Richtlinie verlangt in Artikel 32 Abs. 1 Satz 1 von den Mitgliedstaaten, die zur Umsetzung erforderlichen Rechts- und Verwaltungsvorschriften binnen drei Jahren zu erlassen. Dieser Gesetzgebungsauftrag richtet sich vor allem an den Bundesgesetzgeber, das Bundesdatenschutzgesetz (BDSG) entsprechend zu ändern. Die EU-DSRL bezieht sich nur auf Tätigkeiten, die in den Anwendungsbereich des Gemeinschaftsrechts fallen. Hierzu gehören nicht nur die privatwirtschaftliche Datenverarbeitung, sondern auch große Bereiche der öffentlichen Verwaltung, z. B. im Umwelt-, Wirtschafts- und Verwaltungsverfahrensrecht. Da der Umgang mit personenbezogenen Daten in der öffentlichen Verwaltung in starkem Maße vom allgemeinen Datenschutzrecht geprägt ist, bietet es sich an, den Anforderungen der EU-DSRL durch eine umfassende Änderung des BDSG gerecht zu werden. Dadurch wird auch sichergestellt, daß bei einer Ausweitung der EG-Kompetenzen das BDSG nicht erneut angepaßt werden muß. Soweit bestimmte Bereiche nicht in den Kompetenzbereich der EG fallen, können von der EU-DSRL abweichende Regelungen getroffen werden, bzw. die bestehenden Gesetze können beibehalten werden. Die EU-DSRL macht eine Anpassung des nationalen Datenschutzrechtes auf einem hohen Niveau notwendig. Sie verlangt eine Vielzahl von Verbesserungen des BDSG. Es handelt sich insbesondere um folgende Änderungen:

- Ausweitung des Anwendungsbereichs im nicht öffentlichen Bereich (§ 1 Abs. 2 Nr. 2),
- Aufnahme einer einheitlichen Datenerhebungsregelung auch für den nicht öffentlichen Bereich (§ 6),
- Einführung von Sonderregelungen über die Verarbeitung sog. sensibler Daten (§§ 12, 47),
- Verbot automatisierter Einzelentscheidungen (§ 13),
- Vorabkontrolle und Technikfolgenabschätzung (§ 18 Abs. 2 Satz 2 Nr. 4, § 20),
- Einführung eines allgemeinen Widerspruchsrechts (§ 28),
- Ausweitung der Befugnisse und Verbesserung der Rechtsstellung der Datenschutzkontrollinstanzen (§§ 38, 39, 48, 53),
- Möglichkeit der Erarbeitung von Verhaltensregeln durch Berufsverbände u. ä. (§ 49) und
- Ausweitung des Datenschutzes im Medienbereich (§ 52).

Zweite Zielsetzung: Modernisierung des Datenschutzrechts

Nach 7 Jahren Praxiserfahrung mit den Regelungen des BDSG hat sich gezeigt, daß das Gesetz in vieler Hinsicht konkretisierungs- und verbesserungsbedürftig ist. Dies gilt insbesondere für moderne Verfahren automatisierter Datenverarbeitung, die bei Erarbeitung des BDSG 1990 noch nicht bekannt oder zumindest noch nicht in größerem Umfang eingeführt waren. Die Nutzung des Internets und anderer Kommunikationsnetze, die selbstverständliche Nutzung neuer Datenträgersysteme wie CD-ROM oder Chipkarten, die massenhafte Verwendung von Personalcomputern, beeindruckende Verbesserungen im Bereich der Sicherheitstechnik, insbesondere bei der Kryptografie, führen dazu, daß die derzeit gültigen Regelungen des BDSG, die sich noch an der Großrechnertechnologie der 70er und 80er Jahre orientieren, umfassend überarbeitet werden müssen. Bei dem Einsatz von einigen neuen technischen Verfahren (z. B. Videotechnik, Chipkarten, CD-ROM) greift die bisherige Regelungstechnik des BDSG teilweise völlig ins Leere. Die Folge sind schwerwiegende unsanktionierte Verstöße gegen das Persönlichkeitsrecht und ein großes datenschutzrechtliches Vollzugsdefizit. Erste Vorschläge des Bundesministeriums des Innern (BMI; Referentenentwurf zum BDSG, Stand 14. Januar 1997) beschränken sich, abgesehen von einigen unwesentlichen Korrekturen, auf die Umsetzung der EU-DSRL. Ein solcher Regelungsansatz nimmt billigend in Kauf, daß das Datenschutzrecht immer mehr zum Papiertiger und zur reinen Alibiveranstaltung verkommt. Zudem macht er eine baldige erneute Novellierung des BDSG erforderlich. Dies kann weder im Interesse der Rechtsanwender noch allgemein im Interesse der Rechtssicherheit liegen. Daher verfolgt der vorliegende Gesetzentwurf einen umfassenden Regelungsansatz, bei dem nicht nur die praktizierte Form der Datenverarbeitung, sondern auch absehbare künftige Entwicklungen berücksichtigt werden. Das allgemeine Datenschutzrecht ist in immer größerem Maße verwoben mit dem Telekommunikations- und Medienrecht. Daher lehnt sich der vorliegende BDSG-Entwurf an moderne sonstige Regelungen des Informations- und Kommunikationsrechts an und bezieht sich hierauf.

Es werden insbesondere folgende Anpassungen an den technischen Standard vorgenommen:

- Aufnahme neuer Kriterien bei der Systemgestaltung (Revisionsfähigkeit § 14 Nr. 9, anonyme Nut-

zung § 16 Abs. 1 Satz 2 und 3, Datensparsamkeit § 7 Abs. 3 Nr. 1, § 16 Abs. 2 Satz 1, Pflicht zur Zugriffssicherung § 15 Abs. 2),

- Recht und Pflicht zur Datenverschlüsselung (§ 15 Abs. 1, § 26),
- Einführung des Datenschutz-Audits (§ 17),
- Einführung einer Regelung zur externen Systemwartung (§ 31 Abs. 6),
- Chipkartenregelung (§ 32),
- Regelung der Videoüberwachung (§ 33) und
- Regelung der automatisierten Veröffentlichung personenbezogener Daten (§ 45).

Außerdem werden folgende Verbesserungen des Datenschutzes vorgeschlagen:

- Erweiterung des Schutzzweckes des Gesetzes auf den Grundrechtsschutz allgemein (§ 1 Abs. 1),
- Präzisierung der Zweckbindung (§ 9 Abs. 1 und 2),
- Einschränkung der Datenbeschaffung über Selbstauskünfte (§ 22 Abs. 6),
- Einschränkung der Generalklauseln im öffentlichen Bereich (§§ 35 bis 38),
- spezielle Vorschriften zum Direktmarketing (§ 46 Abs. 2 und 3),
- Regelung des Datenschutzes in Beschäftigungsverhältnissen (§ 50) und
- Einführung von Verbandsbeteiligungen in datenschutzrechtlichen Verfahren (§ 20 Abs. 1 Satz 3, § 49).

Insofern greift der vorliegende Gesetzentwurf die Vorschläge der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-Konferenz) vom 14./15. März 1996 zur „Modernisierung und europäischen Harmonisierung des Datenschutzrechts" auf (abgedruckt in: 16. TB BfD 1995/96 – Drucksache 13/7500 – Anlage 15, vgl. dort auch 1.4 und 2.1.5).

Regelungskonzeption

Die Grundkonzeption des vorliegenden Entwurfes ist: Bewährtes bewahren und Defizite beseitigen. Dies macht es (entgegen den BMI-Vorschlägen) zunächst erforderlich, die Terminologie des BDSG bez. der Verarbeitungsschritte an die Terminologie der meisten Landesdatenschutzgesetze und der EU-DSRL anzupassen. Statt die derzeit schon hochkomplizierte BDSG-Struktur durch eingeflickte Regelungsfetzen noch weiter zu verkomplizieren, wird eine neue Ordnung gewählt. Statt die vollständige Trennung zwischen öffentlichem und nicht öffentlichem Bereich beizubehalten, werden die meisten Regelungen vor die Klammer gezogen. Strukturell geht die EU-DSRL davon aus, daß Datenschutz im öffentlichen und im nicht öffentlichen Bereich nach vergleichbaren Kriterien erfolgt. Dies entspricht auch den technischen Gegebenheiten, die durch das gemeinsame Nutzen von datenverarbeitenden Medien (z. B. Chipkarten, Internet) eine strikte Trennung zwischen öffentlichem und nicht öffentlichem Bereich nicht mehr erlaubt. Ein erwünschter Nebeneffekt dieses Ansatzes ist, daß die Normen überschaubarer, verständlicher, klarer und einheitlich anwendbar werden. Soweit Regelungen überflüssig geworden sind, etwa zum Fehlen von Landesrecht (§ 1 Abs. 2 Nr. 2, § 27 Abs. 1 Nr. 2 Buchstabe b BDSG), zu den inzwischen privatisierten Sondervermögen des Bundes (Bahn, Post, z. B. § 2 Abs. 2 Satz 2 BDSG), wurden diese ersatzlos gestrichen. Soweit Generalklauseln präzisiert werden konnten, ohne daß dies zu Beeinträchtigungen eines sinnvollen ADV-Einsatzes führt, wurden diese im Interesse der Normenbestimmtheit auf das Notwendige eingegrenzt. Dies führte vor allem zur Beseitigung der uferlosen Generalklauseln im öffentlichen Bereich. Vorbildliche Regelungen aus bestehenden Gesetzen, insbesondere aus neueren Landesdatenschutzgesetzen, aus dem Medien- und dem Telekommunikationsrecht, wurden übernommen.

Damit liegt ein Vorschlag vor, der – anders als der Referentenentwurf des BMI vom 14. Januar 1997 – sich auf der Höhe der Zeit bez. der technischen Entwicklung und der juristischen Diskussion befindet. Ein solches Gesetz kann zum Vorbild für Landesregelungen und von Datenschutzrecht in anderen Staaten werden.

Einzelbegründung

Zu § 1 Abs. 1 (Zweck des Gesetzes)

Der bisherige Verweis auf das Persönlichkeitsrecht als ausschließlicher Schutzzweck (§ 1 Abs. 1 BDSG) erfaßt nicht mehr die Regelungsbreite des Datenschutzrechtes und auch nicht die reale Bedrohungssituation durch moderne Datenverarbeitung. Das vom Bundesverfassungsgericht (BVerfG) aus dem Persönlichkeitsrecht (Artikel 2 Abs. 1 i.V. m. Artikel 1 Abs. 1 GG) abgeleitete Recht auf informationelle Selbstbestimmung (BVerfG, NJW 1984, 419 ff.), das in vielen Länderverfassungen ausdrücklich erwähnt wird (z. B. Artikel 4 Abs. 2 LVerf NW, Artikel 33, 34 SächsLVerf), ist der zentrale verfassungsrechtliche Bezugspunkt des BDSG. Daneben haben jedoch fast alle anderen Grundrechte einen informationsrechtlichen Gehalt, allen voran das in Artikel 10 GG geschützte Fernmeldegeheimnis. Von zunehmender Bedeutung ist das Recht auf Gleichbehandlung (Artikel 3 GG), da die Informationstechnik neue personenbezogene Differenzierungs- und damit Diskriminierungsmöglichkeiten eröffnet. Durch den generellen Verweis auf die Grundrechte wird zugleich zum Ausdruck gebracht, daß das BDSG bei Grundrechtskollisionen einen Ausgleich sucht. Derartige Kollisionen bestehen z. B. bei der Presse- und Informationsfreiheit (Artikel 5 GG) oder bei der Berufsfreiheit (Artikel 12 GG).

Zu § 1 Abs. 2 bis 4 (Anwendungsbereich des Gesetzes)

Im öffentlichen Bereich wird der Anwendungsbereich bez. vorübergehender und interner Dateien (§ 1 Abs. 3 BDSG) erweitert. Dies ist von Artikel 3 Abs. 1 EU-DSRL gefordert, wonach es bei einer automatisierten Verarbeitung nicht mehr auf den Dateibegriff ankommt. Außerdem wird die gesamte Ak-

ten-Datenverarbeitung erfaßt. Nur von der Erforderlichkeitsprüfung ausgenommen werden Vorentwürfe und Notizen (§ 9 Abs. 1 Satz 2, bisher § 3 Abs. 3 Satz 2 BDSG).

Bisher orientiert sich der Anwendungsbereich des BDSG, insbesondere im nicht öffentlichen Bereich, am Dateibegriff (§ 1 Abs. 2 Nr. 3, § 27 Abs. 2 BDSG), der in § 3 Abs. 3 BDSG definiert ist. Hierauf kann künftig verzichtet werden, wenn die Umschreibung der Datei in Artikel 2 c EU-DSRL zur Umschreibung des Anwendungsbereichs im nicht öffentlichen Bereich verwendet wird. Angesichts moderner Verarbeitungssysteme wie neuronale Netze, regelbasierte Systeme, Expertensysteme oder objektorientierte Programmierung erweist sich der überkommende Dateibegriff nicht mehr als trennscharf. Die bisherige Formulierung des § 27 BDSG „aus Dateien" wird in der Form übernommen, daß auch die Weiterverarbeitung von Daten, die aus einer strukturierten Sammlung stammen, erfaßt werden. Diese Regelung erfaßt sowohl die Weiterverarbeitung durch die verarbeitende Stelle (Nutzung) wie durch andere Stellen nach einer Übermittlung. Damit wird verhindert, daß durch Übermittlung von Daten vom BDSG geschützte Daten aus dem Schutzbereich herausfallen.

Der Ausschluß persönlicher und privater Datenverarbeitung aus dem Anwendungsbereich in Absatz 2 Satz 1 Nr. 2 entspricht Artikel 3 Abs. 2 dritter Spiegelstrich EU-DSRL.

Mit Absatz 3 (Anwendung auf Stellen in der EU) wird das primäre Ziel der EU-DSRL, den freien Verkehr personenbezogener Daten in der EU nicht zu beschränken (Artikel 1 Abs. 2 EU-DSRL), verwirklicht. Er setzt Artikel 4 EU-DSRL über die Abgrenzung des nationalen Regelungsbereichs in nationales deutsches Recht um. Da der Begriff der Datenverarbeitung auch die Datenerhebung umfaßt, ist das BDSG auch anwendbar, wenn Daten im Inland nur erhoben werden. Niederlassung ist jede auf Dauer angelegte selbständige oder unselbständige Einrichtung zur effektiven und tatsächlichen Ausübung einer Tätigkeit, ungeachtet ihrer Rechtsform.

Die Regelung in Absatz 4 (Verhältnis zu anderen Regelungen) entspricht inhaltlich § 1 Abs. 4 Satz 1 BDSG und erweitert diese auf Regelungen der Europäischen Gemeinschaften (EG). Berufs- und besondere Amtsgeheimnisse, die bisher ungeregelt blieben (§ 1 Abs. 4 Satz 2, § 39 BDSG), werden in das Regelungskonzept des neuen BDSG integriert (vgl. § 12).

Zu § 2 (Öffentliche und nicht öffentliche Stellen)

Die Regelung entspricht weitgehend dem bisherigen § 2 BDSG. Die Formulierung erlaubt gegenüber der bisherigen Rechtslage eine einfachere Abgrenzung. Auf die bisher in § 2 Abs. 2 BDSG vorgenommene Definition der öffentlichen Stellen der Länder wird verzichtet. Diese Definition ist Ländersache. Bisher war die Unterscheidung zwischen öffentlichen und nicht öffentlichen Stellen von großer Bedeutung, da unterschiedliches Recht anzuwenden war. Dies gilt nicht mehr in dem Maße, da für beide Bereiche ein möglichst einheitlicher Datenschutzstandard formuliert wird. Dessenungeachtet bleiben Unterschiede bestehen, da öffentliche Stellen den betroffenen Personen hoheitlich gegenübertreten und gesetzlich präzise definierte Aufgaben wahrnehmen, während nicht öffentliche Stellen mit den betroffenen Personen privatrechtlich auf der gleichen Ebene stehen.

Zu § 3 (Weitere Begriffsbestimmungen)

Die Definition personenbezogener Daten nach Absatz 1 entspricht § 3 Abs. 1 BDSG sowie inhaltlich Artikel 2 a EU-DSRL. Es kommt nicht darauf an, daß die verarbeitende Stelle die Identität der natürlichen Person kennt; ein personenbezogenes Datum ist schon dann anzunehmen, wenn für sie, evtl. mit Hilfe einer anderen Stelle, die Möglichkeit besteht, eine Identifizierung durchzuführen. Daten sind grundsätzlich auch dann personenbezogen, wenn sie einem Pseudonym zugeordnet sind.

Auf die Definition der Akte und der Datei kann wegen der Regelung in § 1 Abs. 2 verzichtet werden. Die ausdrückliche Erwähnung von Bild- und Tonträgern als Beispiele für Aktenverarbeitung (§ 3 Abs. 3 BDSG) ist angesichts der zunehmenden digitalisierten Verarbeitung von Bild und Ton, die regelmäßig den bisherigen Dateibegriff erfüllt, anachronistisch und kann daher ersatzlos entfallen.

Der umfassende Verarbeitungsbegriff des Absatzes 3 entspricht der Terminologie des Artikels 2 b EU-DSRL als auch der meisten Landesdatenschutzgesetze. Dieser ist im Interesse einer möglichst einheitlichen Handhabung anstelle des überkommenen Begriffs des BDSG, der die Erhebung und die Nutzung nicht mit einbezieht (§ 3 Abs. 3 bis 6 BDSG) auch im Bundesrecht zu verwenden. Dies hat zweifellos bei der Revision der spezifischen Datenschutzregelungen im Bundesrecht weitreichende Folgen. Diese Folgen werden durch eine Übergangsregelung in § 56 aufgefangen. Durch die weitere Fassung des Verarbeitungsbegriffs wird zudem die Lesbarkeit des Gesetzes erheblich verbessert.

Der Begriff „Anonymisieren" entspricht § 3 Abs. 7 BDSG.

Der Begriff der „verarbeitenden Stelle" in Absatz 5 entspricht inhaltlich § 3 Abs. 8 BDSG sowie der Definition des „für die Verarbeitung Verantwortlichen" in Artikel 2 d EU-DSRL bzw. des „Auftragsverarbeiters" in Artikel 2 e EU-DSRL.

Der Begriff „Dritter" in Absatz 6 Satz 1 entspricht § 3 Abs. 9 BDSG sowie Artikel 2 f EU-DSRL.

In Artikel 2 g EU-DSRL wird der neue Begriff des „Empfängers" eingeführt. Dieser ist z. B. bei der Beschreibung des Auskunftsanspruchs von Bedeutung (Artikel 12 a EU-DSRL). Zur Klarstellung wird bei der Defintion des Empfängers in Absatz 6 Satz 2 im Klammersatz erläutert, daß der Begriff sowohl den Übermittlungsempfänger als auch den Auftragnehmer bei der Datenverarbeitung im Auftrag erfaßt.

Zu § 4 (Zulässigkeit der Verarbeitung)

Die Regelung entspricht § 4 Abs. 1 BDSG.

Zu § 5 (Einwilligung)

Die Regelung entspricht § 4 Abs. 1 BDSG. In Artikel 2 Buchstabe h EU-DSRL wird besonders betont, daß nur eine ohne Zwang erteilte Einwilligung rechtlich wirksam ist. Sie muß nach Artikel 7 a EU-DSRL „ohne jeden Zweifel" erteilt worden sein (vgl. auch Artikel 26 Abs. 1 Buchstabe a EU-DSRL). Einwilligungen können auch befristet erklärt werden. Die eindeutige Bestimmbarkeit bezieht sich insbesondere auf die Verarbeitungszwecke und die verarbeitenden Stellen (Empfänger), u. U. aber auch auf das Verarbeitungssystem. Bei der Einwilligung kann insofern differenziert werden. Der Hinweis auf die Widerruflichkeit stellt nur eine Klarstellung dar. Bei Widerruf der Einwilligung wird die weitere Verarbeitung grundsätzlich unzulässig.

Auf die Sonderregelung zur Einwilligung im Bereich der wissenschaftlichen Forschung (§ 4 Abs. 3 BDSG) wird verzichtet. Der darin zum Ausdruck kommende Gedanke kann bei der Auslegung der „Angemessenheit" in Satz 2 berücksichtigt bleiben. Der Verzicht auf die Schriftlichkeit der Einwilligung ist gemäß § 51 Abs. 2 Nr. 3 weiterhin schriftlich festzuhalten.

In Absatz 3 wird den modernen technischen Erfordernissen entsprechend neben der schriftlichen die elektronisch erklärte Einwilligung zugelassen. Die Regelung entspricht dem Vorschlag des § 3 Abs. 7 des Entwurfs eines Telekommunikationsdienstedatenschutzgesetzes (TDDSG).

Zu § 6 (Datenerhebung)

Nach Artikel 2 b EU-DSRL wird der Vorgang der Datenerhebung auch im nicht öffentlichen Bereich dem Vorbehalt des Gesetzes unterstellt. Dies ermöglicht eine einheitliche Regelung für nicht öffentliche und öffentliche Stellen. Artikel 10 EU-DSRL fordert die in Absatz 1 Satz 3 vorgesehene Verbesserung der Unterrichtung der von einer Datenerhebung betroffenen Person. Für den Fall, daß die Daten nicht bei der betroffenen Person erhoben werden, erfolgt eine Benachrichtigung nach § 24. Die generelle Erhebungsregelung schließt nicht aus, daß bereichsspezifisch zusätzlich Besonderheiten normiert werden.

Zu § 7 (Verantwortung bei der Datenübermittlung)

Die Regelung entspricht § 15 Abs. 2, § 16 Abs. 2, § 17 Abs. 3 BDSG. Ihr Anwendungsbereich wird auf den privaten Bereich ausgedehnt. Die Verantwortung bei der Übermittlung im automatisierten Abrufverfahren ist in § 30 Abs. 4 geregelt.

Zu § 8 (Datenübermittlung in Drittländer)

Die EU-DSRL macht eine umfassende Neuregelung der Datenübermittlung ins Ausland notwendig. Artikel 1 Abs. 2 EU-DSRL fordert den ungehinderten Datenaustausch innerhalb der EU. In der Regelung werden die Anforderungen der Artikel 25 und 26 EU-DSRL umgesetzt.

Durch Absatz 7 wird sichergestellt, daß die Übermittlung in Drittländer nicht unter erleichterten Bedingungen erfolgen kann als die Übermittlung innerhalb der EU. Außerdem bleiben dadurch verfahrensrechtliche Vorschriften (z. B. die Benachrichtigung gemäß § 37 Abs. 1 Nr. 3 bei Übermittlungen vom öffentlichen in den privaten Bereich) anwendbar.

Zu § 9 (Allgemeine Grundsätze: Zweckbindung, Erforderlichkeit, Datenvermeidung, Datensicherheit, Transparenz)

Es besteht ein Bedürfnis, die grundlegenden Prinzipien des Datenschutzes im Gesetz „vor der Klammer" klarzulegen. Hierauf beziehen sich die weiteren Regelungen des Gesetzes zum Umgang mit personenbezogenen Daten. Sie sind Auslegungsrichtschnur des Gesetzes.

Der Grundsatz der Erforderlichkeit in Absatz 1 Satz 1 ergibt sich aus Artikel 6 Abs. 1 Buchstabe c und e EU-DSRL.

Der Zweckbindung nach den Absätzen 1 und 2 wird eine eigenständige Regelung gewidmet. In Umsetzung des Artikels 6 EU-DSRL wird klargestellt, daß dieser Grundsatz auch im nicht öffentlichen Bereich gilt. Zur Vermeidung einer ausufernden Interpretation des Verarbeitungszwecks wird klargestellt, daß bei der Festlegung des Zwecks neben dem Erhebungs-/Speicherungsgrund auch der Verwendungszusammenhang und das eingesetzte System maßgeblich sind.

Artikel 6 Abs. 1 Buchstabe b EU-DSRL konkretisiert das Zweckbindungsprinzip durch das Verbot unvereinbarer Verarbeitungszwecke und greift damit eine entsprechende Passage des Volkszählungsurteils des BVerfG auf (BVerfG, NJW 1984, 427). Verarbeitungszwecke sind miteinander unvereinbar, wenn das Verfolgen des einen Zwecks dazu führt, daß das Erreichen des anderen Zwecks nicht erreicht werden kann bzw. unvertretbar erschwert wird. Dies ist z. B. der Fall, wenn bei den betroffenen Personen erhobene statistische Planungsdaten für Verwaltungszwecke genutzt werden sollen.

Das Verbot von Persönlichkeitsprofilen (vgl. § 12 Abs. 6 SächsDSG) basiert auf der Rechtsprechung des BVerfG (BVerfGE 27, 6). Damit soll ausgeschlossen werden, daß mit automatisierten Mitteln Daten so zusammengefaßt verarbeitet werden, daß die betroffene Person zum reinen Objekt degradiert und damit ihrer menschlichen Würde beraubt wird.

Der Grundsatz der Datenvermeidung (Absatz 3 Nr. 1) wird erstmalig in das allgemeine Datenschutzrecht aufgenommen.

Die Verantwortlichkeit der verarbeitenden Stelle für die insbesondere in den §§ 14 ff. aufgeführten Maßnahmen der Datensicherheit wird in Absatz 3 Nr. 2 festgelegt.

Transparenz nach Absatz 3 Nr. 3 ist die Grundvoraussetzung für die betroffenen Personen, um zu erfahren, wer wann bei welcher Gelegenheit etwas über sie weiß. Außerdem ist es eine Voraussetzung für die Datenschutzkontrolle und damit für die Durchsetzung datenschutzrechtlicher Vorschriften. Transpa-

renz wird durch eine Vielzahl von Regelungen in diesem Gesetz verwirklicht. Dies sind insbesondere

- die Auskunftspflicht (§ 23),
- die Benachrichtigungspflicht (§ 24),
- Informationspflichten, z. B. bei Einholung einer Einwilligung (§ 5 Satz 3), bei der Datenerhebung (§ 6 Abs. 1), bei beabsichtigten Übermittlungen vom öffentlichen in den privaten Bereich (§ 37 Abs. 1 Nr. 3) beim Einsatz von Chipkarten u. ä. (§ 32 Abs. 4 Satz 1) und
- die neu eingeführte Quittierungspflicht beim Einsatz von Chipkarten u. ä. (§ 32 Abs. 2).

Neben Maßnahmen, die eine Transparenz für die jeweiligen Betroffenen schafft, fordert Artikel 21 Abs. 1 EU-DSRL allgemeine „Maßnahmen, mit denen die Öffentlichkeit der Verarbeitungen sichergestellt wird". Diesem Ziel dienen

- die Meldepflicht, verbunden mit dem Einsichtsrecht in die Meldungen (§ 19),
- die Pflicht der Datenschutzbeauftragten, die bei diesen geführte Übersicht verfügbar zu machen (§ 18 Abs. 4 Satz 2),
- die Veröffentlichung der Ergebnisse und der Begründung von Technikfolgenabschätzungen (§ 20 Abs. 1 Satz 4),
- die Hinweispflicht beim Einsatz von Videoüberwachung (§ 33 Abs. 1 Satz 2),
- die Veröffentlichung eines zweijährlichen Tätigkeitsberichts durch den Bundesbeauftragten (§ 41 Abs. 1) und
- das Einsichtsrecht in das Register automatisierter Veröffentlichungen (§ 45 Abs. 3 Satz 2).

Zu § 10 (Besondere Regelungen zur Zweckbindung)

Absatz 1 entspricht dem bisherigen § 14 Abs. 4, § 31 BDSG, die zusammengefaßt werden. Zu Daten, die der Sicherstellung eines ordnungsgemäßen Betriebes dienen, gehören die Protokolldaten aus lokalen Netzen, Firewalls, Sicherheitsprodukten und z. B., soweit diesen keine weitere Funktion zukommt, Daten, die bei Internet-Providern anfallen.

Zu § 11 (Datengeheimnis)

Die Regelung entspricht § 5 BDSG sowie den Anforderungen des Artikels 16 EU-DSRL. Die bisherige Ausnahme öffentlicher Stellen von der ausdrücklichen Verpflichtung auf das Datengeheimnis wird gestrichen. Auch im öffentlichen Bereich soll die mit der Verpflichtung verbundene Aufklärung der Bediensteten sichergestellt werden.

Zu § 12 (Verarbeitung besonderer Kategorien von Daten)

Artikel 8 EU-DSRL erlaubt die Verarbeitung von besonders sensiblen Daten nur unter engen materiellen Voraussetzungen. Gegenüber den allgemeinen rechtlichen Regelungen ist ein verstärkter materieller und verfahrensrechtlicher Schutz erforderlich. Der Schutz nach Artikel 8 EU-DSRL muß mit dem teilweise sich überschneidenden Schutz von Berufs- und besonderen Amtsgeheimnissen in Einklang gebracht werden. Dies wird dadurch erreicht, daß beiden Datenkategorien ein weitgehend gleichwertiger Schutz zugeschrieben wird. Zugleich werden in Absatz 3 typische allgemeine Offenbarungstatbestände eingeführt, mit denen vermieden werden kann, daß auf die Rechtsfigur des rechtfertigenden Notstands (§ 34 StGB) als Verarbeitungsbefugnisnorm zurückgegriffen werden muß. Absatz 2 stellt aber klar, daß bei Berufs- und besonderen Amtsgeheimnissen ansonsten eine Offenbarung einer gesetzlichen Grundlage bedarf. In jedem Fall gehen spezifische Regelungen vor. Bei deren Erlaß sind die Grenzen des Artikels 8 Abs. 2 bis 4 EU-DSRL zu beachten. Geraten besonders geschützte Angaben an Dritte, so waren sie bisher nicht besonders geschützt. Diese Regelungslücke wird durch Absatz 1 behoben.

Während bei sensiblen Daten, der Vorlage des Artikels 8 Abs. 5 EU-DSRL folgend, eine Zweckänderung durch Rechtsvorschrift möglich ist, ist dies bei Berufs- und besonderen Amtsgeheimnissen – wie bisher (vgl. § 39 Abs. 2 BDSG) – nur durch Gesetz möglich.

Bei öffentlichen Stellen schränkt § 12 die Möglichkeiten der Zweckänderung nach § 35 ein. Bei den nicht öffentlichen Stellen wird die Zweckänderung, wie sie vor allem § 43 Abs. 1 Nr. 2 bis 4 erlaubt, eingeschränkt. Auch bei einer zweckentsprechenden Datenverarbeitung ist aber bei nicht öffentlichen Stellen gemäß § 47 zusätzlich eine Güterabwägung vorzunehmen.

§ 13 (Automatisierte Einzelentscheidungen)

Artikel 15 EU-DSRL fordert ein generelles Verbot automatisierter Einzelentscheidungen, verbunden mit der Möglichkeit, Ausnahmen vorzusehen. Soweit Ausnahmen vorgesehen werden sollen, bedürfen sie einer speziellen gesetzlichen Grundlage.

Zum Zweiten Unterabschnitt (Technische und organisatorische Maßnahmen)

Ergänzend zu den 10 Geboten der Datensicherheit (sog. technische und organisatorische Maßnahmen, vgl. § 9 BDSG mit Anlage) sind weitere technische Regeln nötig, die Datenvermeidung, Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Daten sicherstellen. Auf die 10 Gebote der Datensicherheit, die ursprünglich auf die Großrechnertechnologie vor 20 Jahren ausgerichtet waren, die aber auch bei Kleinrechnern und bei vernetzten Systemen anwendbar sind, kann als Auffangnorm nicht verzichtet werden.

Sie müssen aber weiterentwickelt werden.

Zu § 14 (Standardmaßnahmen)

Es macht keinen Sinn, die technischen und organisatorischen Standardmaßnahmen in einer Anlage des Gesetzes aufzuführen (so bisher Anlage zu § 9 Satz 1 BDSG). Dem Vorbild vieler Landesdatenschutzgesetze folgend (z. B. § 7 Abs. 2 NDSG), werden diese

Maßnahmen in das Gesetz inkorporiert. Die derzeit gültigen Standardmaßnahmen (sog. 10 Gebote) orientieren sich noch in starkem Maße an der Großrechnertechnologie, z. B. indem zwischen Datenträger- und Speicherkontrolle (Eingabe bzw. weitere Verarbeitung) differenziert wird. Daher werden Maßnahmetypen zusammengefaßt.

Regelmäßig erfüllen bestimmte Datensicherungsmaßnahmen mehrere Kontrollzwecke. Überschneidungen bei den Maßnahmen sind zwangsläufig, ja erwünscht. Die allgemeinen Sicherungserfordernisse werden durch Artikel 17 Abs. 1 EU-DSRL vorgegeben.

Mit Nummer 5 wird dem Umstand Rechnung getragen, daß in verarbeitenden Stellen verstärkt mit vernetzten Rechnersystemen gearbeitet wird.

Artikel 17 Abs. 2 und 3 EU-DSRL fordert die Auftragskontrolle nach Nummer 6.

Die unter Nummer 8 neu aufgenommene Verfügbarkeitskontrolle wird von Artikel 17 EU-DSRL verlangt. Schutz vor zufälliger Zerstörung oder Verlust bedeutet z. B. Schutz vor Blitzschlag oder Stromausfall. Geeignete Sicherungsmaßnahmen sind z. B. das Erstellen zusätzlicher Sicherungskopien und deren geschützte Lagerung.

Artikel 17 Abs. 4 EU-DSRL verlangt zum Zweck der Beweissicherung die Dokumentation der datenschutzrelevanten Verfahrenselemente. Dies ist durch die bisherigen 10 Gebote nicht ausreichend sichergestellt. Daher fordert Nummer 9 die Sicherstellung der Revisionsfähigkeit der Datenverarbeitungsverfahren. Revisionsfähigkeit ist die Möglichkeit, technische und organisatorische Abläufe der Datenverarbeitung und Rahmenbedingungen davon den jeweils Verantwortlichen zuzurechnen. Auch dies ist ein Hilfsmittel zur Sicherstellung der Transparenz. Bei der Gestaltung der Hard- und der Software müssen Mittel zur Verfügung stehen, die einen Abgleich des Ist- mit dem Sollzustand ermöglichen. Dies erfolgt durch die vollständige Dokumentation des Systems, die verbindliche Festlegung des Umgangs mit dem System und eine geeignete (automatische) Protokollierung relevanter Systemveränderungen. Die Möglichkeit des Auffindens von Daten, die z. B. bei Expertensystemen oder sonstigen komplexen Datenbanken keine Selbstverständlichkeit ist, wird durch die Revisionskontrolle eingefordert.

Die Organisationskontrolle nach Nummer 10 dient einerseits als Auffangnorm, andererseits erfaßt sie alle nicht technischen Maßnahmen (z. B. Dienstvorschriften, Anweisungen, Bedienungsanleitungen, Zuständigkeitspläne). Auf sie kann im Rahmen der Datensicherung nicht verzichtet werden.

Zu § 15 (Besondere Maßnahmen)

Die Verschlüsselung von Daten bei der Speicherung, aber vor allem bei der Datenübermittlung, wird als besondere Datensicherheitsmaßnahme empfohlen bzw. vorgeschrieben (Absatz 1).

Absatz 2 regelt zwingend die Zugangs- und Zugriffskontrolle (vgl. § 16 Nr. 1). Schutzsoftware ist heute allgemein und mit vertretbarem Kostenaufwand erhältlich. Die Regelung findet beim Einsatz von Personalcomputer in ungesicherten Räumen ebenso Anwendung wie beim Zugang zu öffentlichen Netzen.

Zu § 16 (Grundsätze der Systemgestaltung)

Die Regelung orientiert sich weitgehend am Mediendienste-Staatsvertrag (MD-SV), der sich derzeit im Gesetzgebungsverfahren der Länderparlamente befindet. § 12 Abs. 3 MD-SV verbietet die faktische Erzwingung datenschutzrechtlicher Einwilligungen (Absatz 1 Satz 1). Das Recht zur Inanspruchnahme von anonymen bzw. pseudonymen Nutzungen von Angeboten (Absatz 1 Satz 2) orientiert sich an § 13 Abs. 1 MD-SV. Der Grundsatz der Datensparsamkeit (Absatz 2 Satz 1) ist in § 12 Abs. 5 MD-SV enthalten. Es ist leider immer wieder festzustellen, daß Datenverarbeitungssysteme so ausgestaltet sind, daß sie den Anforderungen des Datenschutzrechts nicht entsprechen (z. B. Unmöglichkeit, bestimmte Daten zu löschen oder zu sperren, ungenügende Protokollierung, vgl. z. B. XIII. TB LfD Nds. 1995/96, 44, 70). Daher wird eine ausdrückliche Überprüfungspflicht der technischen Verfahren auf deren Vereinbarkeit mit dem Recht festgelegt (Absatz 2 Satz 2). Hierbei kann auf externen Sachverstand zurückgegriffen werden (Absatz 2 Satz 3, vgl. Datenschutz-Audit: § 17).

Zu § 17 (Datenschutz-Audit)

Das Datenschutz-Audit verfolgt das Ziel, datenschutzfreundliche Produkte auf dem Markt zu fördern, indem deren Datenschutzkonzept geprüft und bewertet wird. Eine entsprechende Regelung zum Datenschutz-Audit enthält § 17 MD-SV. Das Instrument des Datenschutz-Audits läßt sich dadurch fördern, daß bewertete Produkte bei der Anschaffung vorgezogen werden (§ 16 Abs. 2 Satz 2).

Zu § 18 (Behördlicher bzw. betrieblicher Datenschutzbeauftragter)

Soweit von Melderegelungen Abstriche gemacht werden, verpflichtet Artikel 18 Abs. 2 zweite Alternative EU-DSRL zur Bestellung von betrieblichen oder behördlichen Datenschutzbeauftragten. Diesen obliegt die „unabhängige Überwachung" des Datenschutzes. Da Datenschutzbeauftragte öffentlicher Stellen oft zugleich betriebliche Datenschutzbeauftragte nach den §§ 36, 37 BDSG sind, sollte das BDSG eine einheitliche Vorgabe enthalten. Die Konzeption zum betrieblichen Datenschutzbeauftragten hat sich bewährt und wird übernommen.

Bei einer Betriebsgröße von mehr als 500 EDV-Beschäftigten ist im Interesse einer ausreichenden Präsenz die Bestellung eines eigenen Mitarbeiters als Datenschutzbeauftragter notwendig, der für diese Tätigkeit freigestellt wird. So soll ausgeschlossen werden, daß die Bestellung zum reinen Alibi wird. Ist die Aufgabe des Datenschutzbeauftragten nicht von einer einzelnen Person zu bewältigen, so ist nicht ausgeschlossen, daß dem Datenschutzbeauftragten weitere unterstützende Personen zugeordnet werden (Absatz 4 Satz 3).

Absatz 1 Satz 1 stellt sicher, daß nicht nur bei der Berufung eines sog. internen, sondern auch eines externen (d. h. nicht betriebsangehörigen) Datenschutzbeauftragten die Mitbestimmungsregelung greift. Der Begriff „Vertretung der Beschäftigten" erfaßt sowohl den Personalrat von öffentlichen Stellen wie den Betriebsrat in der Privatwirtschaft. Besteht keine Vertretung der Beschäftigten, so entfällt die Mitbestimmung.

Der Datenschutzbeauftragte erhält ein Beratungsrecht und eine entsprechende Pflicht bez. der Auswahl von Verarbeitungsverfahren sowie – Artikel 20 Abs. 2 EU-DSRL folgend – Aufgaben bei der Vorabkontrolle. Das Einsichtsrecht in die beim Datenschutzbeauftragten zu führende Systemübersicht wird in Artikel 21 Abs. 3 EU-DSRL zwingend vorgeschrieben. Neben Absatz 1 Satz 1 stellt auch Absatz 3 Satz 3 klar, daß personelle Entscheidungen zum Datenschutzbeauftragten mitbestimmungspflichtig sind. Die Entbindungsregelung des § 36 Abs. 3 Satz 3 BDSG, die in der Praxis viele Unklarheiten zur Folge hat, wird durch eine klarere Regelung ersetzt, die auch sog. „externe" Datenschutzbeauftragte erfaßt.

Zu § 19 (Meldepflicht)

Die Regelung ersetzt die Norm zum Dateienregister beim Bundesbeauftragten in § 26 Abs. 5 BDSG sowie die Meldepflicht nach § 32 BDSG für nicht öffentliche Stellen gegenüber der Aufsichtsbehörde. Die Meldepflicht wird auf das von Artikel 18, 19 EU-DSRL geforderte Maß beschränkt. Artikel 19 Abs. 1 Buchstabe d und e EU-DSRL fordert eine Erweiterung der im Rahmen der Meldepflicht zu machenden Angaben.

Zur Führung des in Absatz 3 erwähnten Registers bei den Datenschutzkontrollinstanzen und zur Gewährung der Einsichtnahme durch jedermann verpflichtet Artikel 21 Abs. 2 EU-DSRL.

In einer Rechtsverordnung, die gemäß Artikel 80 Abs. 2 GG der Zustimmung des Bundesrates bedarf, werden die näheren Voraussetzungen der Meldepflicht festgelegt. Hierbei sind insbesondere gemäß Artikel 18 Abs. 2 erster Spiegelstrich EU-DSRL die Verarbeitungskategorien festzulegen, bei denen unter Berücksichtigung der zu verarbeitenden Daten und der sonstigen Umstände eine Beeinträchtigung der Grundrechte unwahrscheinlich ist.

Zu § 20 (Vorabkontrolle durch Technikfolgenabschätzung)

Artikel 20 EU-DSRL fordert eine Vorabkontrolle, wie sie schon heute in § 7 Abs. 3 NDSG als einzigem deutschen Datenschutzgesetz vorgesehen ist. Wegen der bisher aufgetretenen Probleme bei der Anwendung des § 7 Abs. 3 NDSG und im Hinblick auf die Vorgabe der EU wird die Formulierung zur Technikfolgenabschätzung modifiziert. Außerdem wird erstmals im deutschen Datenschutzrecht, dem Umwelt- und dem Verbraucherschutzrecht folgend, die Einführung einer Verbandsbeteiligung vorgesehen. Bei Verfahren, von denen keine spezifischen Risiken ausgehen, wird die Vorabkontrolle durch den Datenschutzbeauftragten gemäß § 18 Abs. 2 Nr. 4 durchgeführt.

Zu § 21 (Unabdingbarkeit)

Die Regelung entspricht § 6 Abs. 1 BDSG.

Zu § 22 (Sicherung der Betroffenenrechte)

Es entstehen immer mehr Dateien, an denen mehrere Stellen beteiligt sind. Typisch ist diese Konstellation bei Chipkartenanwendungen. Die Betroffenen laufen hier Gefahr, bei der Wahrnehmung ihrer Rechte nicht den richtigen Ansprechpartner zu finden, da für sie nicht überschaubar ist, wer verarbeitende Stelle ist. Daher wird § 6 Abs. 2 BDSG (vgl. auch neuerdings z. B. § 4 Abs. 2 BrDSG) in Absatz 1 inhaltlich übernommen.

Immer wieder ist festzustellen, daß verarbeitende Stellen, gegenüber denen Betroffene ihre Rechte direkt oder über den Landesbeauftragten für den Datenschutz geltend machen, die streitbefangenen Daten löschen, um sich einer Auskunft, einer Beanstandung oder auch einem Schadensersatz zu entziehen. Obwohl Gerichte festgestellt haben, daß eine solche Löschung unzulässig ist, weil Grund zur Annahme besteht, daß Betroffenenbelange beeinträchtigt werden, findet diese Praxis weiterhin statt. Es bedarf daher der eindeutigen ausdrücklichen Regelung des Absatzes 2.

Zu § 23 (Auskunft an die betroffene Person)

Artikel 12 a dritter Spiegelstrich EU-DSRL verlangt die in Absatz 1 enthaltene Erweiterung des Auskunftsanspruchs. Die Regelungen des § 19 und des § 34 BDSG werden zusammengefaßt.

Die Auskunftsverweigerung soll die Ausnahme bleiben. Daher werden die Gründe, weshalb eine Auskunft unterbleiben kann, in Absatz 3 eng begrenzt.

Entgegen dem bisherigen § 34 Abs. 5 BDSG soll die Auskunftserteilung immer unentgeltlich sein. Ein geringes Entgelt bei wirtschaftlicher Nutzungsmöglichkeit wird derzeit nur von der Bundes-Schufa verlangt. Damit soll vermieden werden, daß sich im Auskunftsgeschäft interessierte Stellen bei Bonitätsprüfungen von den betroffenen Personen Selbstauskünfte vorlegen lassen, statt eine direkte Auskunft einzuholen. Die bisherige komplizierte Entgeltregelung ist aber wegen ihrer geringen tatsächlichen Bedeutung überflüssig. Durch Absatz 6 wird der Mißbrauch durch Selbstauskünfte eingeschränkt. Außerdem besteht für die verarbeitenden Stellen die Möglichkeit, durch die Gestaltung der Auskunft (z. B. Weglassen der Namensangaben) die wirtschaftliche Nutzbarkeit einzuschränken bzw. auszuschließen.

Mit Absatz 6 soll verhindert werden, daß sich Stellen gespeicherte Daten über die betroffene Person beschaffen, die sich in einer Zwangslage (z. B. anläßlich des Abschlusses eines Wohnungs-, Versicherungs- oder Arbeitsvertrags) befinden.

Zu § 24 (Benachrichtigung)

Die Benachrichtigung nach den Absätzen 1 und 2 ergibt sich zwingend aus Artikel 11 EU-DSRL. Sie ersetzt die bisherige Regelung in § 33 BDSG. Absatz 2 Nr. 6 ist eine zwingende Folgeregelung zu § 45.

Immer wieder ereignen sich Fälle, in denen die verarbeitende Stelle die Unzulässigkeit ihrer Datenverarbeitung feststellt, ohne daß die betroffenen Personen hierüber informiert werden, auch wenn für diese ein Schaden droht oder entstanden ist, z. B. im Bereich der Personaldatenverarbeitung. Hier müssen die Betroffenen in den Stand gesetzt werden, ihre Rechte wahrzunehmen, so wie dies § 19 DSG MV vorsieht (Absatz 3). Die Unterrichtungspflicht sollte nicht Dritten (z. B. den Datenschutzkontrollinstanzen), sondern der verarbeitenden Stelle auferlegt werden.

Zu § 25 [Datenkorrektur (Berichtigung, Sperrung, Löschung)]

Der Begriff der Datenkorrektur wird im Interesse der vereinfachten Lesbarkeit des Gesetzes eingeführt. Die Regelung faßt entsprechend dem Auftrag von Artikel 12 b EU-DSRL die bisherigen §§ 20 und 35 BDSG zusammen und entschlackt sie von überflüssigen Ausnahmeregelungen. Der Anspruch auf Berichtigung nach Absatz 1 faßt die Regelungen des § 20 Abs. 1, § 35 Abs. 1 BDSG zusammen. Er realisiert die Pflicht der verarbeitenden Stellen nach Artikel 6 Abs. 1 Buchstabe d EU-DSRL. Der Anspruch auf Löschung nach Absatz 2 faßt die Regelungen des § 20 Abs. 2, § 35 Abs. 2 BDSG zusammen und realisiert die entsprechende Pflicht nach Artikel 6 Abs. 1 Buchstabe e EU-DSRL. Die Aktenregelung in § 20 Abs. 1 und 5 BDSG wird in Absatz 4 zusammengefaßt und präzisiert.

Die Regelung zur Benachrichtigung von Empfängern zum Zweck der Datenkorrektur (Nachbericht) in Absatz 5 basiert auf Artikel 12 c EU-DSRL.

Zu § 26 (Recht auf Datensicherung)

Seit langem wird eine kontroverse Debatte darüber geführt, inwieweit die Bürgerinnen und Bürger die Befugnis haben, die ihnen verfügbaren technischen Datensicherungsmaßnahmen einzusetzen. Teilweise wird die Ansicht vertreten, daß die Sicherungsmaßnahmen nur so stark sein dürfen, daß sie von Sicherheitsbehörden durchbrochen werden können. Eine solche Regelung, deren tatsächliche Umsetzung faktisch nicht überwach- und durchsetzbar ist, hätte zwangsläufig zur Folge, daß faktisch auch kein Schutz vor Angriffen durch Dritte möglich wäre. Datensicherungsmaßnahmen können nicht künstlich auf einen bestimmten Stand festgeschrieben werden, da die rasante technische Entwicklung hierüber hinweggehen würde. Es wird ein subjektives Recht auf Datensicherung festgeschrieben. Davon unberührt bleibt die gesetzliche Befugnis von Sicherheitsbehörden, Datenträger zu beschlagnahmen oder die Datenkommunikation abzuhören.

Zu § 27 (Anrufung der Datenschutzkontrollinstanz)

Die Regelung entspricht § 21 Satz 1 BDSG und wird erweitert auf den Bereich der Aufsichtsbehörden. Sie entspricht den Anforderungen des Artikels 28 Abs. 4 Satz 1 und 2 EU-DSRL.

Zu § 28 (Widerspruchsrecht)

Artikel 14 a EU-DSRL sieht dieses Recht auf Widerspruch gegen Maßnahmen der Datenverarbeitung vor.

Zu § 29 (Schadensersatz)

Artikel 23 EU-DSRL macht die Haftung bei rechtswidriger Datenverarbeitung weder von der Anwendung eines automatisierten Verfahrens noch von der nach § 823 BGB erforderlichen Schuldhaftigkeit abhängig. Die bestehenden Schadensersatzregelungen (§§ 7, 8 BDSG) werden entsprechend angepaßt, wobei auch nicht mehr zwischen öffentlichen und nicht öffentlichen Stellen unterschieden wird. Aus Sicht der Geschädigten ist es unerheblich, ob eine durch Datenverarbeitung bedingte Schädigung durch eine Behörde oder durch Private erfolgt. Außerdem wird die Pflicht zum Ersatz eines immateriellen Schadens im Gesetz festgelegt, ohne daß eine schwere Verletzung des Persönlichkeitsrechtes nachgewiesen werden müßte (Absatz 1 Satz 2). Die Regelung ist geeignet, die verarbeitenden Stellen zur Rechtmäßigkeit anzuhalten. Bisher war es den Betroffenen oft äußerst schwer, einen materiellen Schaden bzw. einen schwerwiegenden immateriellen Schaden nachzuweisen. Dies ist nach § 29 nicht mehr nötig.

Zu § 30 (Einsatz automatisierter Abruf- und Verbundverfahren)

Die Regelung entspricht § 10 BDSG. Neben den herkömmlichen Abrufverfahren gibt es immer mehr Verbundverfahren, bei denen mehrere Stellen in einem gemeinsamen Datenbestand die Verarbeitung personenbezogener Daten durchführen. Die Regelung wird auf diese ebenso riskante Verfahrensart ausgeweitet.

Die Benennung einer Stelle, gegenüber der Betroffenenrechte insgesamt geltend gemacht werden können (Absatz 2 Satz 2 Nr. 2), erleichtert den betroffenen Personen die Übersicht und die Durchsetzung ihrer Rechte (vgl. § 22 Abs. 1). Die gerichtliche Geltendmachung der Rechte hat gegenüber der verarbeitenden Stelle bzw. den verarbeitenden Stellen zu erfolgen.

Zu § 31 Abs. 1 bis 4 (Auftragsverarbeitung)

Die Regelung entspricht dem § 11 BDSG. Sie setzt die Vorgaben der Artikel 16 und 17 Abs. 2 und 3 EU-DSRL um. Die gegenüber § 11 Abs. 3 Satz 2 BDSG verschärfte Hinweispflicht in Absatz 3 Satz 2 basiert auf der Erfahrung, daß der Auftragnehmer regelmäßig überlegene Kenntnisse bez. der technischen Voraussetzungen der Datenverarbeitung als auch bez. des Datenschutzrechts hat. Es soll gewährleistet wer-

den, daß der Auftraggeber über mögliche Rechtsverstöße auch tatsächlich hingewiesen wird.

Zu § 31 Abs. 5 (Externe Wartung)

Die rechtliche Einordnung der externen Wartung bzw. Systembetreuung durch eine andre als die verarbeitende Stelle ist bis heute rechtlich umstritten. Daher bedarf es einer Klarstellung. Diesem Bedürfnis wurde z. B. in Brandenburg nachgekommen (§ 11a BbgDSG). Es wird sichergestellt, daß geeignetes Personal eingesetzt und eine Kontrollmöglichkeit eröffnet werden. Der Formulierungsvorschlag orientiert sich am Tendenzpapier des von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 1993 beauftragten Gesprächskreises (XII. TB LfD Nds., S. 277; vgl. 15. TB LfD Bremen, S. 11f.). Die Regelung erlaubt im Rahmen der Erforderlichkeit auch die Kenntnisnahme von besonders sensiblen Daten. Die Daten unterliegen einer strengen Zweckbindung (§ 10 Abs. 1). Die hierbei tätigen Personen unterliegen dann als Hilfspersonen der Geheimhaltungspflicht (Berufsgeheimnis, Datengeheimnis). Ein Verstoß hiergegen führt für sie als Hilfspersonen (§ 203 Abs. 3 StGB) sowie als datenverarbeitende Personen (§ 54) zur strafrechtlichen Verantwortlichkeit.

Zu § 32 (Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien)

Die neue Chipkartentechnologie wirft datenschutzrechtliche Probleme auf, auf die das aktuelle Datenschutzrecht keine Antwort gibt. Es ist daher eine neue Regelung erforderlich, die die datenschutzrechtliche Verantwortlichkeit aller Beteiligten festlegt und den einzelnen vor unfreiwilliger Preisgabe seiner Daten schützt. Die Regelung gewährt im Interesse informationeller Selbstbestimmung für die Betroffenen ein Mindestmaß an Transparenz, Freiwilligkeit und die Wahlmöglichkeit einer anonymen Alternative. Chipkarten sind nur die am stärksten verbreitete Technologie von mobilen Speicher- und Verarbeitungsmedien, die automatisiert mit Lese- und Schreibgeräten kommunizieren. Andere Beispiele sind sog. Smart Cards oder „Persönliche Digitale Assistenten". Die Regelung versucht, absehbare technische Entwicklungen mit zu berücksichtigen (vgl. 16. TB BfD 1995/96, 1.4).

Es war bisher unklar, wer beim Chipkarteneinsatz als verarbeitende Stelle anzusehen ist. Dies wird in Absatz 1 klargestellt. In Absatz 2 wird eine Quittierungspflicht in das Gesetz aufgenommen. Elektronische Systeme sind niemals fehlerfrei. Den betroffenen Personen muß die Möglichkeit gegeben werden, Verarbeitungsfehler nachzuweisen. Diese Notwendigkeit besteht vor allem, wenn die Betroffenen durch die elektronische Form der Datenerhebung keinen sonstigen Nachweis, z. B. in Form eines Formulars oder eines Antrags, vorliegen haben oder wenn die Datenerhebung gar keine bewußte Mitwirkungshandlung der Betroffenen erfordert.

Beim Chipkarteneinsatz gibt es regelmäßig eine größere Anzahl von verarbeitenden Stellen. Es ist den betroffenen Personen nicht zuzumuten, ihr Auskunftsrecht einzeln gegenüber jeder dieser Stellen geltend zu machen. Daher sieht Absatz 3 ein konzentriertes Verfahren vor. Zugleich muß sichergestellt werden, daß über die Wahrnehmung des Auskunftsrechtes nicht andere als die betroffene Person und die verarbeitende Stelle von der Datenspeicherung Kenntnis erlangen.

Wegen der Flüchtigkeit des Speicherungsvorgangs bei mobilen Kleinrechnern besteht die Gefahr, daß das Einholen der Einwilligung nur noch zu einer technisch vollzogenen Formsache wird. Um dies zu verhindern, muß von der Speicherung eine umfassende Information der Betroffenen erfolgen. Die Freiwilligkeit wird durch ein Diskriminierungsverbot bei Nichtnutzung von mobilen Kleinrechnern sichergestellt (Absatz 4).

Zu § 33 (Videoüberwachung)

In ihrer Entschließung hat die DSB-Konferenz am 14./15. März 1996 generelle Regelungen zur Videoüberwachung angemahnt. Die Regelung entspricht inhaltlich weitgehend § 32 LDSG SH und § 33c BbgDSG. Es soll gewährleistet werden, daß die durch Videotechnik erfolgende optische Überwachung öffentlicher Räume eingegrenzt wird. Die Norm differenziert zwischen der reinen Erhebung (Beobachtung) und der anschließenden Speicherung. Eine akustische Überwachung als andersartiger und zumeist schwerwiegenderer Eingriff bleibt ohne ausdrückliche gesetzliche Regelung unzulässig (vgl. 16. TB BfD 1995/96, 1.4).

Zu § 34 (Anwendungsbereich)

Absatz 1 ist identisch mit § 12 Abs. 1 BDSG; Absatz 2 ist identisch mit § 12 Abs. 3. Die Regelung des § 12 Abs. 2 wurde durch Erlaß von Landesdatenschutzgesetzen obsolet. § 12 Abs. 4 wird durch die spezielle Regelung der Datenverarbeitung bei Beschäftigungsverhältnissen (§ 50) überflüssig.

Zu § 35 (Zulässigkeit der Verarbeitung)

Die Regelung ersetzt den bisherigen § 14 BDSG. Der Gehalt des § 14 Abs. 1 BDSG ist nunmehr in § 9 Abs. 1 geregelt. § 14 Abs. 2 BDSG war wegen seiner Unbestimmtheit verfassungsrechtlicher Kritik ausgesetzt. Entsprechend den Vorgaben von Artikel 7a bis f EU-DSRL erfolgt eine präzise bestimmte, eingegrenzte Regelung, wie sie auch in einigen Ländern besteht (vgl. § 10 Abs. 2 NDSG). Bei der Datenerhebung ist zusätzlich § 6 zu beachten.

Zu § 36 (Übermittlung innerhalb des öffentlichen Bereichs)

Die Regelung ersetzt § 15 BDSG. Dessen Absatz 2 (Verantwortlichkeit) findet sich in § 7 sowie in § 30 Abs. 4 (automatisiertes Abrufverfahren) wieder. Dessen Absatz 3 (Zweckbindung) wird ersetzt durch § 9 Abs. 1. Auf eine Übermittlungssonderregelung an öffentlich-rechtliche Religionsgesellschaften (§ 15

Abs. 4 BDSG) kann verzichtet werden. Derartige Religionsgesellschaften gelten als nicht öffentliche Stellen (§ 2 Abs. 4 S. 2). Einen praktischen Bedarf für eine § 15 Abs. 4 BDSG entsprechende Regelung besteht neben speziellen Regelungen (z. B. im Melde- und im Steuerrecht) nicht.

Absatz 2 (verbundene personenbezogene Unterlagen) entspricht § 15 Abs. 5 BDSG.

Absatz 3 (Weitergabe innerhalb einer öffentlichen Stelle) entspricht § 15 Abs. 6 BDSG. Eine Datenweitergabe innerhalb einer öffentlichen Stelle ist wie eine Übermittlung zu bewerten. Eine derartige Regelung hat sich bei Landesdatenschutzgesetzen als notwendig und praktikabel erwiesen (vgl. z. B. § 11 Abs. 4 NDSG).

Zu § 37 (Übermittlung an Empfänger außerhalb des öffentlichen Bereichs)

Die Regelung ersetzt § 16 BDSG. Die dort enthaltenen weiten Voraussetzungen werden in Absatz 1 nach dem Vorbild von Landesdatenschutzgesetzen (vgl. z. B. § 13 NDSG) eingeschränkt. § 16 Abs. 2 BDSG wird in § 7 Satz 1 geregelt. Absatz 2 entspricht § 16 Abs. 4 BDSG.

Zu § 38 (Rechtsstellung)

Die Regelung ersetzt die überdetaillierten §§ 22 f. BDSG. Zur Sicherstellung der nach Artikel 28 Abs. 1 EU-DSRL geforderten Unabhängigkeit der Kontrollstelle wird der Bundesbeauftragte und seine Dienststelle aus dem Bundesministerium des Innern (bisher § 22 Abs. 5 BDSG) ausgelagert und verselbständigt. Eine Abs. 1 entsprechende Regelung enthält § 22 Abs. 2 BerlDSG.

Zu § 39 (Kontrolle durch den Bundesbeauftragten)

Artikel 28 Abs. 3 erster Spiegelstrich EU-DSRL fordert für die Kontrollstelle umfassende Untersuchungsbefugnisse. Angesichts der zunehmenden Automatisierung sind angemessene Zugangsmöglichkeiten für den Bundesbeauftragten sicherzustellen. Dazu gehört auch, daß online bzw. automatisiert verfügbare personenbezogene Datenbestände außerhalb der verarbeitenden Stelle überprüft werden können (Absatz 2).

Zu § 40 (Beanstandung durch den Bundesbeauftragten)

Die Regelung entspricht § 25 BDSG. Das Instrument der Beanstandung, verbunden mit der Möglichkeit, die Öffentlichkeit über Datenschutzverstöße zu informieren (vgl. § 26 Abs. 1 BDSG), hat sich bei der Datenschutzkontrolle in der Bundesrepublik Deutschland bewährt. Es handelt sich hierbei um eine „wirksame Einwirkungsmöglichkeit" im Sinne von Artikel 28 Abs. 3 zweiter Spiegelstrich EU-DSRL.

Zu § 41 (Weitere Aufgaben und Befugnisse des Bundesbeauftragten)

Die Regelung ersetzt § 26 BDSG. Artikel 28 Abs. 2 EU-DSRL verlangt eine Absatz 3 entsprechende Anhörung der Kontrollstelle auch vor dem Erlaß von Rechts- und Verwaltungsvorschriften. Absatz 4 ermöglicht die Kooperation der zuständigen Datenschutzbehörden.

Zu § 42 (Anwendungsbereich)

Die Regelung entspricht § 27 BDSG unter Berücksichtigung des in § 1 Abs. 2 und 3 definierten und ausgeweiteten Anwendungsbereichs.

Zu § 43 (Verarbeitung für eigene Zwecke)

Die Regelung ersetzt die Regelung des § 28 BDSG. Wesentliche materielle Veränderungen erfolgen nicht. Durch einen überschaubaren Aufbau wird die Anwendung erheblich erleichtert. Absatz 1 Nr. 1 setzt Artikel 7b EU-DSRL um. Absatz 1 Nr. 2 findet seine Entsprechung in Artikel 7e und f EU-DSRL. Da die listenmäßige Datenverarbeitung nach § 28 Abs. 2 Satz 1 Nr. 1 Buchstabe b BDSG, die auf eine begrenzte Privilegierung des einfachen Adressenhandels bzw. des Direktmarketing abzielt, in diesen Bereichen praktisch völlig ihre Bedeutung verloren hat, wird diese Regelung gestrichen. Bezüglich der äußerst problematischen Nutzung für Zwecke der Werbung und der Markt- und Meinungsforschung (bisher § 28 Abs. 3 BDSG) erfolgt eine Sonderregelung in § 46. Auf die Forschungsregelung in § 28 Abs. 1 Satz 1 Nr. 4 und Abs. 2 Nr. 2 BDSG konnte wegen der neuen Regelung des § 51 Abs. 2 Satz 1 Nr. 3 verzichtet werden. Absatz 2 entspricht § 28 Abs. 4 BDSG.

Zu § 44 (Geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung)

Die Regelung ersetzt inhaltlich unverändert § 29 BDSG. Auf die Regelung zur listenmäßigen Verarbeitung (§ 29 Abs. 2 Satz 1 Nr. 1 Buchstabe b BDSG) wird verzichtet, da diese Regelung ihre frühere praktische Relevanz verloren hat und diese Alternative lediglich als eine Konkretisierung der bisherigen Nummer 1 Buchstabe a angesehen werden kann.

Zu § 45 (Automatisierte Veröffentlichung)

Die Datenübermittlung an eine unbestimmte Zahl von Dritten stellt aus der Sicht des Datenschutzes eine völlig neue Qualität dar gegenüber Einzelübermittlungen. Derartige Übermittlungen erfolgen zunehmend in automatisierter Form, z. B. auf CD-ROM, Disketten oder in automatisiert abrufbaren Verzeichnissen im Internet oder von Online-Diensten. Obwohl hierbei regelmäßig gegen die Vorschriften der §§ 29, 33 BDSG verstoßen wird, expandiert der Markt solcher Veröffentlichungen (vgl. § 3 Abs. 3 Nr. 5) bisher ungehindert. Statt den dauernden Gesetzesverstoß hinzunehmen oder durch ein Verbot ein Ausweichen von Anbietern ins Ausland zu ermuntern, zielt die

Regelung darauf ab, die Veröffentlichung einerseits zuzulassen, zugleich aber geeignete Datenschutzmechanismen zu installieren. Die Regelung korrespondiert mit den neuen Vorschriften im Telekommunikationsrecht (§ 89 Abs. 8 TKG, § 10 TDSV). Grundlage ist ein Einwilligungsmodell (sog. „opt in"). Da damit jedoch wegen der Unüberschaubarkeit der Weiterverarbeitung und wegen der faktischen Wirkungslosigkeit eines Widerrufs der Einwilligung aufgrund erfolgter Weiterübermittlungen für die Betroffenen die informationelle Selbstbestimmung verlorengehen kann, wird dieses Modell durch eine individuelle wie auch eine generelle Widerspruchsmöglichkeit ergänzt (sog. „opt out"). Der individuelle Widerspruch erfolgt gegenüber der verarbeitenden Stelle (Absatz 4), während der generelle Widerspruch über eine beim Bundesbeauftragten geführte Widerspruchsliste erfolgt, die vor der Veröffentlichung abgeglichen werden muß (Absatz 2). Damit wird die vom Deutschen Direktmarketing Verband (DDV) initiierte Idee der „Robinsonliste" auf eine verbindliche Basis gestellt. Über das vom Bundesbeauftragten zu führende Verzeichnisregister können sich die Bürgerinnen und Bürger darüber informieren, wo u. U. Daten über sie verarbeitet werden. Dies schafft die für die Betroffenen notwendige Transparenz, die aus tatsächlichen Gründen mit einer Benachrichtigung allein nach § 24 Abs. 1 nicht mehr erreicht werden kann.

Zu § 46 (Datenverarbeitung zum Zweck der Werbung und der Markt- und Meinungsforschung)

Die Regelung ersetzt den bisherigen § 28 Abs. 3 BDSG und erweitert ihn, soweit sich in der Praxis Vollzugsdefizite erwiesen haben (vgl. XIII. TB LfD Nds. 1995/96, 154 f.). Dabei wird ein der elektronischen Veröffentlichung vergleichbares Instrumentarium zum Einsatz gebracht. Insofern kann auf die Begründung zu § 45 verwiesen werden. An die Stelle der Widerspruchsliste tritt die Werbestoppliste. Es bedarf der Differenzierung zwischen diesen beiden Listen, da den Betroffenen die Wahlmöglichkeit gegeben werden muß, einerseits über elektronische Verzeichnisse ihre Erreichbarkeit sicherzustellen bzw. zu unterbinden, andererseits Werbung zu erhalten bzw. davon verschont zu bleiben. Die Regelung der Absätze 1 und 2 setzt Artikel 14 b EU-DSRL um (vgl. 16. TB BfD 1995/96, 1.4).

Die Information der beworbenen Personen schafft für diese die erforderliche Transparenz. Der Hinweis auf das Widerspruchsrecht wird von Artikel 14 Satz 2 EU-DSRL gefordert.

Absatz 4 enthält den wesentlichen Regelungsgehalt des bisherigen § 30 BDSG.

Zu § 47 (Verarbeitung besonderer Kategorien von Daten)

Die Regelung stellt, vergleichbar mit § 28 Abs. 2 Satz 2 BDSG klar, daß bei bestimmten Datenkategorien (sog. sensible Daten) der Verarbeitung grundsätzlich schutzwürdige Interessen der Betroffenen entgegenstehen. Damit wird dem Schutzgedanken des Artikels 8 EU-DSRL entsprochen. Davon unberührt bleibt die begrenzte Zulässigkeit der Datenübermittlung bzw. Zweckänderung nach § 12.

Zu § 48 (Aufsichtsbehörde)

Aufsichtsbehörden sind Datenschutzkontrollinstanzen gemäß § 3 Abs. 7 und Kontrollstellen im Sinne von Artikel 28 EU-DSRL. Die nach Artikel 28 Abs. 3 EU-DSRL geforderten Untersuchungsbefugnisse sind in den Absätzen 2 und 3 geregelt, die „wirksamen Einwirkungsbefugnisse" in Absatz 4. Die bisherige völlige Sanktionslosigkeit bei materiell-rechtlichen Datenschutzverstößen konnte nicht beibehalten werden. Insofern wird sowohl ein Feststellungsrecht (Absatz 4 Satz 1 Nr. 2) als auch bei Nichtbeseitigung des Mangels ein Untersagungsrecht (Absatz 4 Satz 2) eingeführt. Als weitere Einwirkungsbefugnisse – zugleich „Klagerecht" bzw. Anzeigebefugnis im Sinne der EU-DSRL – besteht die Möglichkeit der Verfolgung als Ordnungswidrigkeit (§ 55) als auch die der Einschaltung der Strafverfolgungsbehörden (§ 53).

Um eine möglichst effektive Datenschutzkontrolle zu gewährleisten, nehmen Landesbeauftragte für den Datenschutz seit mehreren Jahren in Hamburg, Bremen und Niedersachsen auch die Aufgaben der Aufsichtsbehörde im nicht öffentlichen Bereich nach § 38 BDSG wahr. Diese Zusammenfassung des Datenschutzes in einer Hand hat sich bewährt (XII. TB LfD Nds. 1993/94, S. 233 ff.). Diesen Vorbildern schließen sich andere Länder an (z. B. seit August 1995 Berlin). Hinzu kommt, daß die Landesbeauftragten im höheren Maße die von Artikel 28 Abs. 1 Satz 2 EU-DSRL geforderte „völlige Unabhängigkeit" aufweisen als Teile eines Ministeriums oder einer Bezirksregierung/eines Regierungspräsidiums. Dessenungeachtet bleibt im Rahmen der EU-Vorgaben die Kompetenz der Länder bestehen, die die zuständigen Aufsichtsbehörden selbst bestimmen (Absatz 5 Satz 3; bisher § 38 Abs. 6 BDSG). Für die Länder bietet es sich aber an, die Aufgaben der Aufsichtsbehörden den unabhängigen Landesbeauftragten für den Datenschutz zu übertragen.

Zu § 49 (Verhaltensregeln)

Artikel 27 EU-DSRL sieht vor, daß die Mitgliedstaaten und die Kommission die Ausarbeitung von Verhaltensregeln unterstützen und daß Entwürfe den zuständigen Stellen vorgelegt und von diesen geprüft werden können.

Zu § 50 (Datenverarbeitung bei Beschäftigungsverhältnissen)

Seit Jahren ist unstreitig, daß es eines spezifischen Gesetzes zur Regelung des Arbeitnehmer-Datenschutzes bedarf (vgl. Bundesregierung, Drucksache 12/2948). Inzwischen gibt es im Beamtenrecht Regelungen zum Datenschutz. Ein Arbeitnehmer-Datenschutzgesetz steht aber weiterhin aus. Die Regelung enthält einige wesentliche Aussagen zu diesem Bereich. Sie orientieren sich an entsprechenden Regelungen der Landesdatenschutzgesetze (z. B. § 25

NDSG). Die Norm soll als Übergangsregelung bis zur Verabschiedung eines umfassenden Gesetzes verstanden werden.

Zu § 51 (Datenverarbeitung zum Zweck wissenschaftlicher Forschung)

Die EU-DSRL regelt an verschiedenen Stellen eine Sonderbehandlung der Datenverarbeitung für wissenschaftliche Forschungszwecke (z. B. Artikel 6 Abs. 1 Buchstabe e Satz 2, Artikel 11 Abs. 2, Artikel 13 Abs. 2). Die bisher in § 4 Abs. 3, § 14 Abs. 2 Nr. 9, § 28 Abs. 1 Satz 1 Nr. 3 und Abs. 2 Nr. 2, § 40 BDSG verstreuten Regelungen werden zusammengeführt und dadurch einfacher handhabbar. Wesentliche materielle Änderungen ergeben sich hieraus nicht. § 51 entspricht der Regelung der meisten Landesdatenschutzgesetze (z. B. § 25 Abs. 2 Nr. 3 NDSG), so daß bei länderübergreifenden Forschungsprojekten weitgehend einheitliche Standards beachtet werden müssen.

Bei der Regelung wissenschaftlicher Forschung ist neben den Grundrechten der Betroffenen die Forschungsfreiheit gemäß Artikel 5 Abs. 3 GG zu beachten. Dem wird die Abwägungsklausel in Absatz 2 Nr. 3 gerecht.

Zu § 52 (Datenverarbeitung durch die Medien)

Artikel 9 EU-DSRL sieht eine Privilegierung der Verarbeitung personenbezogener Daten vor, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt. Diese Abweichungen und Ausnahmen dürfen sich aber nur auf Fragen der Zulässigkeit, der Information der betroffenen Person und der Einschränkung der Auskunft beziehen. Derartige Einschränkungen kommen auch nur insofern in Betracht, „als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen".

Diesen Anforderungen genügt der bisherige § 41 BDSG nicht. Abgesehen von der grundlosen Privilegierung von Adressen- und vergleichbaren Verzeichnissen mit journalistischen Anteilen werden die Medien bisher vom Datenschutz, abgesehen von der Gewährleistung der Datensicherheit, fast völlig freigestellt.

Die Privilegierung des § 52 bezieht sich nur auf die journalistisch-redaktionelle Datenverarbeitung. Die Verarbeitung der Medienunternehmen in Verwaltungsangelegenheiten richtet sich nach den allgemeinen Grundsätzen. An die Stelle der Datenschutzkontrollinstanz tritt ein Medien-Datenschutzbeauftragter, dessen Ausgestaltung sich am betrieblichen bzw. behördlichen Datenschutzbeauftragten orientiert. Dieser Mechanismus einer internen Kontrolle hat sich bisher bewährt.

Entsprechend der zwingenden Regelung des Artikels 12 i.V. m. Artikel 9 EU-DSRL wird in Absatz 3 eine Auskunftsregelung übernommen, die den Regelungen bestehender Mediengesetze entspricht.

Die derzeitige Praxis der zeitlich unbegrenzten elektronischen Veröffentlichung von Medienarchiven verstößt gegen den auch im journalistischen Bereich zu beachtenden Grundsatz, daß es eine „Gnade des Vergessens" geben müsse. Diesen Grundsatz hat das BVerfG ausdrücklich in seiner Lebach-Entscheidung betont (BVerfG, NJW 1973, 1226). Daher wird der Zugang zu Pressearchiven und die sonstige Veröffentlichung bei Berichten, die älter als fünf Jahre sind, in Absatz 4 eingegrenzt. Dies schließt jedoch die Nutzung im privaten Bereich ebenso wenig aus als die Nutzung dieser Archive, wenn ein berechtigtes Interesse besteht.

Zu § 53 (Unterrichtung der Staatsanwaltschaft)

Datenschutzstrafrecht spielte bisher keine wesentliche Rolle bei der Durchsetzung des Rechts auf informationelle Selbstbestimmung. Schon bisher war es unbestritten, daß die Kontrollstellen die Befugnis haben, die Strafverfolgungsbehörden über möglicherweise strafbare Sachverhalte zu unterrichten. In Ermangelung einer ausdrücklichen Regelung und angesichts der zwingenden Vorschrift des Artikels 28 Abs. 3 dritter Spiegelstrich EU-DSRL wird dies nun ausdrücklich festgestellt. Mit dieser Regelung steht auch dem Bundesbeauftragten eine „Anzeigebefugnis" zu.

Zu § 54 (Strafvorschriften)

Artikel 28 Abs. 3 dritter Spiegelstrich EU-DSRL fordert Sanktionsmöglichkeiten bei Datenschutzverstößen. Diese müssen jedoch nicht strafrechtlicher Art sein. Daher verfolgt § 54 – dem Vorbild von Landesregelungen folgend (z. B. § 28 NDSG) – eine Entkriminalisierung weniger schwerwiegender Datenschutzverstöße. Diese bleiben als Ordnungswidrigkeit (§ 55) verfolgbar. Als völlig unangemessene Verfolgungsvoraussetzung wird das in § 43 Abs. 4 BDSG normierte Antragserfordernis gestrichen. Datenschutzverstöße verletzen nicht nur Individualrechtsgüter bzw. die individuellen Grundrechte, sondern stellen regelmäßig auch eine Beeinträchtigung öffentlicher Belange dar. Zudem hat die kurze Antragsfrist und die Unkenntnis der Betroffenen von dieser Frist immer wieder dazu geführt, daß wegen Fristablaufs auch schwerwiegende Verstöße nicht verfolgt werden konnten. Der Strafrahmen von § 43 Abs. 3 wird beibehalten.

Zu § 55 (Ordnungswidrigkeiten)

Soweit Datenschutzverstöße nicht mehr strafbar sind, werden sie nach Absatz 1 Nr. 1 und 2 zur Ordnungswidrigkeit. Der Bußgeldrahmen wird angesichts der möglichen Bedeutung der Verstöße gegenüber § 44 Abs. 2 BDSG von 50 000 DM auf 100 000 DM hochgesetzt.

Zu § 56 (Übergangsvorschrift)

Die Übergangsregelung ist notwendig, da mit der Novellierung des BDSG nicht zugleich die gesamten bereichsspezifischen Bundesregelungen überarbeitet werden können, die sich noch an der alten Terminologie des BDSG 1990 orientieren.

Druck: Bonner Universitäts-Buchdruckerei, 53113 Bonn
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28/3 82 08 40, Telefax: 02 28/3 82 08 44
ISSN 0722-8333