Stichworte zum Bundesdatenschutzgesetz

Grundgedanken der gesetzlichen Regelung des Datenschutzes

Rechtsstand: August 2006 (mit 1. Bürokratieabbaugesetz)

Version 2.61 © Harry Zingel 2001-2006, EMail: HZingel@aol.com, Internet: http://www.zingel.de

Inhaltsübersicht

1. Die drei Aspekte des Datenschutzes ... 1
2.1. Gesetzesübersicht ... 1
2.2. Grundlegende Regelungsinhalte ... 1
2.3. Die Rechte der Betroffenen ... 2
2.4. Die Institutionen des Datenschutzrechts ... 2
2.5. Die Meldepflicht ... 2
2.6. Das Datenschutzaudit ... 3
3. Betriebliche Organisation des Datenschutzes ... 3
4. Probleme der grundsätzlichen Rechtsauslegung ... 4
4.1. Geheimhaltungs-Paranoia ... 4
4.2. Datenschutz oder Service-Wüste? ... 4
4.3. Vom Niedergang des Datenschutzes ... 5
4.4. Von Freiheit und Diktatur ... 5
Anhang: Technische und organisatorische Maßnahmen ... 6

1. Die drei Aspekte des Datenschutzes

Die mit dem deutschen Wort „Datenschutz“ korrespondierenden englischen Begriffe

- *Privacy*,
- *Safety* und
- *Security*

lassen den Inhalt des Datenschutzbegriffes wesentlich anschaulicher werden:

Wir können diese drei Begriffe in der folgenden Art und Weise visualisieren.

Dieses Skript befaßt sich ausschließlich mit den rechtlichen Vorschriften zum Datenschutz, die teilweise dem Privacy- und teilweise dem Security-Aspekt aber weniger dem Safety-Aspekt des Datenschutzes angehören. Zusätzlich stehen die Skripte zu „Datenschutz und Kryptographie.pdf“ und „Datenschutz und Sicherheit.pdf“ auf der BWL CD zur Verfügung.

Die umfassende Bedeutung des Datenschutzbegriffes anschaulich demonstriert:

Schutz vor Einsicht Dritter (z.B. Sichtschutz):
Privacy

Sicherheit gegen Unfälle oder Pannen (z.B. Airbag, ABS):
Safety

Schutz vor Einbruch, Diebstahl, Vandalismus oder Kriminalität (z.B. Panzerglas, Wegfahrsperre, Sicherheitsschlösser usw.):
Security

Privacy ist jede Form des Schutzes gegen unbefugte Einsicht Dritter, etwa Codierung oder Signatur von Daten.

Security ist der Schutz gegen Sabotage oder kriminelle Akte, etwa Computerviren, trojanische Pferde oder andere Arten der Spionage.

Safety ist der Schutz vor Datenverlust durch technische Ausfällen von Datenverarbeitungsanlagen etwa durch Datensicherung.

2. Das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) ist die wesentliche Rechtsquelle zum Thema Datenschutz in Deutschland. Es stammt zunächst vom 20.12.1990 und wurde zuletzt im Mai 2001 weitgehend neu gefaßt und erheblich erweitert. Der hier dargestellte Rechtsstand umfaßt nur noch diese Neuregelung, die allerdings weitgehend inkrementell war, d.h., bestehende Regelungen erweiterte und um neue Vorschriften ergänzte aber nur selten grundlegend änderte.

2.1. Gesetzesübersicht

Allgemein regelt das BDSG die folgenden datenschutzrechtlich relevanten Tatbestände (Gesetzesgliederung):

- §§1 bis 11: Allgemeine und grundlegende Regelungen wie Geltung, Grundsatz der Datensparsamkeit und Datenvermeidung, Datengeheimnis, Technische und organisatorische Maßnahmen des Datenschutzes, Meldepflichten usw.
- §§ 12 bis 18: Rechtsgrundlagen der Datenverarbeitung durch öffentliche Stellen
- §§19 bis 21: Rechts des Betroffenen gegenüber öffentlichen Stellen
- §§22 bis 26: Bundesbeauftragter für den Datenschutz
- §§27 bis 31: Rechtsgrundlagen der Datenverarbeitung der nichtöffentlichen Stellen
- §§33 bis 35: Rechte der Betroffenen gegenüber nichtöffentlichen Stellen
- §§38, 38a: Aufsichtsbehörde und
- §§39 bis 46: Sonder-, Straf- und Schlußbestimmungen.

2.2. Grundlegende Regelungsinhalte

Das BDSG gilt für öffentliche und für nichtöffentliche Stellen. Es regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 4 Abs. 1 BDSG), die nur aufgrund des BDSG oder mit Einwilligung des Betroffenen zulässig ist. Dabei schreibt der im Mai 2001 neu in das Gesetz eingefügte Grundsatz der Datensparsamkeit

und Datenvermeidung (§3a BDSG) vor, daß Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten haben, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere muß wo möglich anonymisiert werden.

Für die Übermittlung und Nutzung von Daten sind zahlreiche, zumeist recht restriktive Vorschriften gegeben (z.B. §4b BDSG), von denen allerdings zahlreiche Ausnahmen bestehen. Insbesondere sind in §4c BDSG die Nutzung von Daten im Rahmen von Strafverfahren, zur Abwicklung von Verträgen, bei „wichtigem öffentlichen Interesse“ wie etwa geheimdienstlicher Ermittlung, lebenswichtigem Interesse der Betroffenen und zahlreichen anderen Gründen ausdrücklich ausgenommen; auch existieren in den Gesetzen, die die Tätigkeit der Behörden und Organisationen mit Sicherheitsaufgaben regeln, viele Ausnahmen vom „normalen“ Datenschutz.

2.3. Die Rechte der Betroffenen

Das BDSG regelt die folgenden unabdingbaren Rechte der Betroffenen gegenüber öffentlichen Stellen:

- Auskunft an den Betroffenen über die gespeicherten Daten (§19 BDSG),
- Benachrichtigung über Speicherung von Daten ohne Kenntnis des Betroffenen (§19a BDSG),
- Berichtigung, Löschung und Sperrung von Daten (§20 BDSG),
- Widerspruch gegen die Speicherung (§20 BDSG) und
- Anrufung des Bundesbeauftragten für den Datenschutz (§21 BDSG),
- Schadensersatz bei Verletzung von Persönlichkeitsrechten (§§7, 8 BDSG).

Die Rechte des Betroffenen sind gegenüber nichtöffentlichen Stellen in ähnlicher Form wie die Rechte gegenüber öffentlichen Stellen geregelt:

- Benachrichtigung des Betroffenen über Datenspeicherung und Übermittlungsempfänger (§33 BDSG),
- Auskunft an den Betroffenen hinsichtlich der gespeicherten Daten (§34 BDSG) und
- Berichtigung, Löschung und Sperrung von Daten (§35 BDSG),
- Schadensersatz bei Verletzung von Persönlichkeitsrechten (§§7, 8 BDSG).

Die Rechte des Betroffenen auf Auskunft und auf Berichtigung, Löschung oder Sperrung können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden (sogenannte unabdingbare Rechte; §6 BDSG). Die Schadensersatznorm ist ein *lex specialis* zu den allgemeinen schadensersatzrechtlichen Normen der §§823ff BGB.

Diese tiefgreifenden Rechte werden jedoch durch spezielle Rechtsvorschriften eingeschränkt oder außer Kraft gesetzt. Dies hat zur Folge, daß das Datenschutzrecht zwar theoretisch ein sehr scharfes und wirksames Recht ist, es aber faktisch eine Menge Löcher aufweist. So haben Banken gemäß §24c Kreditwesengesetz (KWG) Kundendaten für die Aufsichtsbehörde zum anonymen Abruf (!) bereitzuhalten. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) kann also auf alle Kontodaten zugreifen, ohne daß die Bank weiß, wann, was über wen abgerufen wird, und ohne daß der Kunde also informiert werden kann. Ab 2005 ist auch eine Amtshilfe zwischen der BaFin und anderen Behörden wie den Finanzämtern oder den Sozialämtern und Arbeitsagenturen festgelegt, so daß diese ebenfalls Zugriff erhalten.

Das Bankgeheimnis des §30a Abgabenordnung (AO) ist damit faktisch abgeschafft worden.

2.4. Die Institutionen des Datenschutzrechts

Das BDSG kennt zwei wesentliche Institutionen:

- Der Bundesbeauftragte für den Datenschutz (§§22 bis 26) ist für den Datenschutz bei öffentlichen Stellen zuständig.
- Öffentliche und nichtöffentliche Stellen ernennen einen Beauftragten für den Datenschutz (§4g BDSG), was jedoch nur noch vorgeschrieben ist, wenn wenigstens 20 Personen in der jeweiligen Stelle mit der Datenverarbeitung beschäftigt sind (nichtöffentliche Stellen: mehr als 9 ständig beschäftigte Arbeitnehmer) (§4f Abs. 1 Satz 3 BDSG).

Institutionen und Einrichtungen des Datenschutzes

Bundesbeauftragter für den Datenschutz (§22)

Gewählt vom Bundestag auf Vorschlag der Bundesregierung (§22 Abs. 1), Verpflichtet mit Eidesformel (§22 Abs. 2) auf fünf Jahre (§22 Abs. 3), keine entgeltlichen Nebentätigkeiten (§23 Abs. 2). Zeugnisverweigerungsrecht (§23 Abs. 4), Schweigepflicht (§23 Abs. 5), weitreichende Kontrollrechte in öffentlichen Stellen (§24) und Verpflichtung zu Beanstandung bei Feststellung von Rechtsverstößen (§25), ferner Bericht an den Bundestag (alle zwei Jahre, §26 Abs. 1), Erstellung von Gutachten (§26 Abs. 2), Empfehlungsrecht (§26 Abs. 3) und Mitwirkung in öffentlichen Stellen (§26 Abs. 4) sowie ein Register geführter Dateien (§26 Abs. 5).

Beauftragter für den Datenschutz (§36)

Nunmehr gleichermaßen zuständig für öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten und damit in der Regel mindestens 20 Arbeitnehmer ständig beschäftigen (§4f Abs. 1), Fachkundeerfordernis und Zuverlässigkeit (§4f Abs. 2), dem Inhaber, Vorstand oder Geschäftsführer unmittelbar unterstellt (§4f Abs. 3), Schweigepflicht (§4f Abs. 4) und umfassende Unterstützung seiner Arbeit (§4f Abs. 5). Wirkt auf Einhaltung des BDSG hin (§4g Abs. 1), überwacht die ordnungsgemäße Datenverarbeitung und macht die beteiligten Personen mit den Vorschriften vertraut (§4g Abs. 1 Nrn. 1 und 2).

Die Ausführung des BDSG wird nunmehr von einer Aufsichtsbehörde kontrolliert, die weitreichende Kontroll- und Einsichtsbefugnisse besitzt (§§36-38a BDSG).

2.5. Die Meldepflicht

Verfahren automatisierter Datenverarbeitung sind vor ihrer Inbetriebnahme zu melden (Meldepflicht). Die zu meldenden Inhalte sind in der eindrucksvollen Liste des §4e BDSG niedergelegt:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach §9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Diese Meldepflicht entfällt jedoch, wenn die meldepflichtige Stelle einen Beauftragten für den Datenschutz bestellt hat (§4d Abs. 2 BDSG) oder nur bis zu vier Arbeitnehmer bei der Erhebung, Verarbeitung und Nutzung von Daten beschäftigt und die Datenverarbeitung ausschließlich für eigene Zwecke erfolgt (§4d Abs. 3 BDSG). Diese neu eingefügte Vorschrift nimmt einerseits die Kleinunternehmen von der Meldepflicht aus, soll aber andererseits die Bestellung von Datenschutzbeauftragten auch ohne Rechtspflicht fördern.

2.6. Das Datenschutzaudit

Zusätzlich zu diesen Vorschriften wurde das Datenschutzaudit als zusätzliche Maßnahme der Zertifizierung des Datenschutzkonzeptes in das Gesetz eingefügt. Hierbei wird eine Überprüfung und Zertifizierung des Datenschutzkonzeptes und der Datensicherheit bei Anbietern von Datenverarbeitungssystemen und -programmen sowie datenverarbeitenden Stellen durch einen unabhängigen Gutachter vorgenommen. Rechtsgrundlage hierfür ist der ab Mai 2001 neu in das Bundesdatenschutzgesetz eingefügten §9a BDSG. Zertifizierungsgegenstand ist hierbei immer das Gesamtkonzept, das auch aber nicht ausschließlich die technischen Aspekte umfassen kann. Die Zertifizierungsergebnisse können veröffentlicht und als besonderes Gütesiegel u.a. auch in der Werbung der Unternehmen verwendet werden. Offensichtlich führt der Gesetzgeber hier ein neues Qualitätsmerkmal in das Datenschutzrecht ein, der die Verbreitung von Maßnahmen des Datenschutzes verbessern soll.

3. Betriebliche Organisation des Datenschutzes

Das Datenschutzgesetz stellt umfangreiche Anforderungen an den praktischen betrieblichen Ablauf der Datenverarbeitung. Diese technisch-organisatorischen Maßnahmen sind in §9 BDSG geregelt und sind nur insoweit erforderlich als der mit den Maßnahmen erforderliche Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht (§9 BDSG). Dabei empfiehlt es sich, die vom Gesetz vorgeschriebenen Maßnahmen als Teil eines Datenschutz-Gesamtkonzeptes zu verstehen, daß neben dem reinen Privacy-Aspekt auch Security- und Safety-Aspekte in sich faßt, also die grundlegenden Forderungen des Gesetzes übersteigt.

In diesem Skript wird nur der rechtliche Teil betrachtet; für die weitergehenden Aspekte stehen eigene Schriftwerke zur Verfügung.

Grundzüge eines umfassenden betrieblichen Datenschutzkonzeptes finden sich in der Anlage zu §9 BDSG:

Anlage zu §9 Satz 1 (Erläuterungen und Ergänzungen in *Kursivdruck*):

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
   - *Sicherung der Eingangsbereiche durch verschlossene Türen;*
   - *Festlegung zugangsberechtigter Personen und Ausgabe von Berechtigungsausweisen oder Schlüsseln.*
2. zu verhindern, daß Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
   - *Einführung und Durchsetzung einer wirkungsvollen Kennwortpolitik;*
   - *Chipkarten oder vergleichbare Benutzerausweise;*
   - *Erzwingen regelmäßiger Änderungen von Kennwörtern;*
   - *Abschalten von Systemen bei Erkennung unberechtigter Zugriffsversuche;*
   - *Voraussetzung ist die Zutrittskontrolle (vorstehend).*
3. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und daß personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

- *Festlegung der jeweils erforderlichen Berechtigungen für jeden Nutzer.*
- *Festlegung von verantwortlichen Stellen für Datenbestände und Festlegung der Genehmigung weiterer Auswertungen durch andere Stellen;*
- *Protokollierung von Job-Aufträgen mit Programm- und Dateibenutzungen;*
- *Verwendung elektronischer Signaturen und kryptographischer Technologien;*
- *Voraussetzung ist die Zugangskontrolle (vorstehend).*

4. zu gewährleisten, daß personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und daß überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
   - *Verwendung elektronischer Signaturen und kryptographischer Technologien;*
   - *Festlegung von Zugriffsberechtigungen, insbesondere durch Kennwörter, Chipkarten oder dgl.;*
   - *Dokumentation des Aufrufes und der Nutzung von Clients, die der Datenübermittlung dienen;*
   - *Protokollieren aller Datenübertragungsprozesse und insbesondere der hierbei verwendeten Systemkennungen (IP-Nummern).*

5. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
   - *Maschinelle Protokollierung von Dateneingaben;*
   - *Vorgabe von Eingabe- und Prüfanweisungen;*
   - *Anweisungen über die Vergabe, Änderung, Löschung und Verwendung von Benutzerzulassungen und Passwort-Regelungen;*
   - *Differenzierung von Zugriffsberechtigungen auf Daten und Programme nach Bearbeitungsart, Modus, Dateninhalten, Zeit und ähnlichen Kriterien.*

6. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
   - *Festlegung von Regelung der Kompetenzen für Auftragserteilung und Auftragsannahme;*
   - *Festlegung von Regelung der Auftragsabwicklung.*

7. zu gewährleisten, daß personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
   - *Regelmäßige Durchführung Datensicherungen auf Medien, die nach einem anderen technischen Prinzip funktionieren (z.B. Festplatten auf optische Datenträger);*
   - *Räumliche Trennung von Datenverarbeitungsanlage und Aufbewahrung der Datensicherung;*
   - *Führung sequentieller Datensicherungen (mehrere frühere Stände);*
   - *Redundanz von Systemen (z.B. RAID-Systeme).*

8. zu gewährleisten, daß zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
   - *Sachliche und organisatorische Trennung von Datenbanken, die für unterschiedliche Zwecke erhoben und/oder geführt werden;*
   - *Möglichkeit der Vergabe Berechtigung für einzelne Tabellen und Felder in einer Datenbank schaffen.*

4. Probleme der grundsätzlichen Rechtsauslegung

Wie wichtig die vorstehenden Regeln sind, sollte offensichtlich sein; dennoch wundert die oft sehr lockere Auslegung selbst durch staatliche Stellen. So waren selbst die Gutscheine zum Krankentransport mit Taxen für Arbeitslosengeld-II-Empfänger zu Anfang so ausgelegt, daß die Taxifahrer die ärzlichen Befunde auf den Gutscheinen (!) einsehen konnten (und Arbeitgeber mußten auf den Hartz-IV-Antragsformularen das Arbeitsentgelt bescheinigen, so daß sie auch über den Antrag selbst Angehöriger ihrer Arbeitnehmer informiert wurden). Neben solchen Extremen findet man oft auch sehr kundenunfreundliche Auslegungen des Datenschutzrechtes: so geben Banken oft keine Auskunft, ob beispielsweise fünf- oder gar dreistellige (!) Kontonummern wirklich existieren, obwohl wer dies fragt ein berechtigtes Interesse haben kann, will er beispielsweise eine Lastschrift buchen. Eine Auskunft wäre also im Interesse des Kunden, denn wird versucht, eine Lastschrift auf ein nichtexistentes Konto auszuführen, weil sich der Kunde beispielsweise beim Ausfüllen der Bestellung vertippt hat, kassieren die Banken kräftig ab. Manche Banken sind bei solchen Anfragen kooperativ, andere wie beispielsweise kürzlich die Sparda-Bank, sind es nicht, und berufen sich dabei regelmäßig auf den Datenschutz. Aber haben sie damit auch Recht?

4.1. Geheimhaltungs-Paranoia

Fälle wie den Vorstehenden kann vermutlich jeder berichten. So bezeichnete im Forum für Betriebswirtschaft ein Teilnehmer meine Ankündigung der Herausgabe der IP-Nummern von Leuten, die einer Straftat verdächtig sind, als widerrechtlich - unter Berufung auf den Datenschutz. Vor vielen Jahren hatte ich einer Person in Africa ein Lufthansa-Ticket bezahlt, und wollte diese Person dann in Frankfurt abholen. Da mein Besucher aber zuvor ca. 1 Woche auf einem LKW zum dortigen Flughafen anreisen mußte (und daher den Flug leicht hätte verpassen können, denn es gibt dort keine Straßen, nur Buschpisten, die sich bei Regen in bodenlosen Matsch verwandeln), wollte ich von der Lufthansa wissen, ob mein Gast sich wirklich an Bord befindet - und auch diese Auskunft wurde mir unter Berufung auf Datenschutzgründe verweigert, so daß ich auf Verdacht nach Frankfurt fahren mußte (und seither die Lufthansa boykottiere). Aber sind solche Auskunftsverweigerungen rechtens?

Wenig bekannt scheint zunächst zu sein, daß das Datenschutzrecht nur für die Verarbeitung personenbezogener Daten gilt. Die Bekanntgabe einer IP-Nummer (z.B. 62.180.101.20), durch die aber nur ein Computer (und keine Person) im Netz identifiziert werden kann, ist damit ebensowenig ein Datenschutzverstoß wie die Veröffentlichung des im Netz zugehörigen Maschinennamens (http://www.bwl-bote.de). Erst die Offenlegung eines bestimmten Nutzers, also eines Menschen wäre datenschutzrelevant - aber darum ging es gar nicht. Bei personenbezogenen Informationen gibt es in der Tat einen Geheimhaltungsgrundsatz, weswegen die einleitend erwähnte Sparda-Bank mir ganz sicher Auskünfte über den Kontostand anderer Personen verweigern kann (und sollte). Oft wird aber ignoriert, daß Betroffene auch einen Anspruch auf Offenlegung von personenbezogenen Daten haben: der Lieferant, dem ein (möglicherweise fehlerhafter) Lastschriftauftrag erteilt wurde, ist damit ebenso ein „Betroffener“ wie derjenige, der für jemand anders ein Flugticket bezahlt hat und nun wissen will, ob dieses Ticket auch benutzt worden ist. Hier müßten also Auskünfte erteilt werden - aufgrund der §§6, 19 und 34 Bundesdatenschutzgesetz (BDSG). Warum werden sie aber dennoch so oft verweigert?

4.2. Datenschutz oder Service-Wüste?

Heute kaum noch bekannt ist, daß bei der Telekom (oder ihrem Vorgänger, der Bundespost) der Ausweis der angerufenen Nummern im Zusammenhang mit Telefonnummern erst seit ca. Mitte der 90er Jahre möglich ist - zuvor wurde selbst der Ausweis der erbrachten Leistungen unter ganz offensichtlich vorgeschobenen Datenschutzbedenken verweigert. Man mußte auf die Rechnung einfach vertrauen. Es steht der Verdacht im Raum, daß man sich hier eine lästige Arbeit am Kunden sparen wollte - genau wie der Lufthansa- oder der Bankmitarbeiter im Verdacht stehen, es mit dem Kundendienst nicht so ernst zu nehmen. Sind Datenschutzbedenken also oft nur vorgeschoben, um den Service nicht verbessern zu müssen?

Interessant ist auch, daß das Datenschutzgesetz offenbar nur so radikal ausgelegt wird, wenn es für einen Mitarbeiter zu Arbeitsminimierung führt - nicht aber wenn es darum geht, die Rechte des Betroffenen wirklich zu schützen. So wird die einst als TCPA und heute als NGSCB bekannte Technik zur Überwachung von Software und PC-Nutzern und zur Zensur von Inhalten ungehindert weiter ausgebaut, und die ersten „sicheren“ PCs sind schon auf dem Markt - wo doch gerade hier in die Rechte der Betroffenen massiv eingegriffen wird. Auch die Bedenken der Datenschützer gegen Kameras in Innenstädten und die Erfassung von Maut-Daten, die sehr leicht zu einem persönlichen Bewegungsprofil zusammengestellt werden können, scheinen den Staat nicht weiter zu interessieren, so wenig wie die Proteste gegen die neuen Überwachungsvorschriften im Steuerrecht, weshalb wir Überwachung und Kontrolle als wahre Motive identifiziert haben.

4.3. Vom Niedergang des Datenschutzes

Datenschutz ist eine wichtige Sache, aber leider zutiefst verkommen und verrottet. Offensichtlich kann der Staat nämlich unter dem Vorwand der Terrorbekämpfung, der Planetenretterei, der Software-Piraterie, des Kindersex im Internet, des allgemeinen ökologistischen Gutmenschentums oder weiß-Gott-was-noch problemlos immer neue Überwachungsnormen institutionalisieren, und den bekanntermaßen schläfrigen deutschen Michel scheint das nichtmal zu beunruhigen. In Handel, Wirtschaft und Dienstleistung dagegen wird der Datenschutz immer mehr zweckentfremdet, Leistungen nicht erbringen zu müssen oder einzuschränken: das Datenschutzrecht ist damit zu einem Servicewüsten-Recht geworden, und hat seinen ursprünglichen Zweck des Schutzes eines staatsfreien, unbeobachteten und autonomen Handelns längst verloren. Das Datenschutzrecht wurde damit pervertiert. Eine grundlegende Reform des Datenschutzes ist damit dringend notwendig, aber dann müßte man eine Menge schöne Dinge wie den Zertifikatehandel, die Maut, die neue Personenkennziffer, NGSCB und am Ende sogar die Spionage der Aliierten Siegermächte („Echolon“) abschaffen. Und das werden Leute wie Trittin oder unser Terroristenanwalt Schily gewiß verhindern.

4.4. Von Freiheit und Diktatur

Der Datenschutz war einst als Freiheitsrecht gedacht, als Recht des Individuums auf informationelle Selbstbestimmung und Freiheit vor Schnüffelei des Staates. Es ist schon erstaunlich, daß in der praktischen Umsetzung genau das Gegenteil daraus geworden ist. Der Staat schnüffelt heute mehr denn je, und von informationeller Selbstbestimmung kann angesichts von Maut, Personenkennziffern und Inhaltskontrolle der Internet-Kommunikation kaum mehr die Rede sein - dafür dient das Datenschutzrecht dazu, dem Einzelnen Auskünfte über seine eigenen, ihn angehenden Angelegenheiten zu verweigern. Wie sehr ein an sich gutgemeintes Gesetz damit in sein Gegenteil verkehrt wurde, ist doch immerhin erstaunlich. Kein Wunder übrigens, daß das Informationsfreiheitsgesetz, das einen umfassenden Auskunftsanspruch gegenüber Behörden regeln soll, seit Jahren auf Eis liegt...

BWL-Bote

Kapitel 4 ist zuerst am 10.04.2004 unter „Datenschutz, das mißverstandene Recht“ im BWL-Boten erschienen: http://www.bwl-bote.de/20040410.htm

Anhang: Technische und organisatorische Maßnahmen
für Datensicherheit und Datenschutz im BDSG:

Die „Gebote für Datensicherheit und Datenschutz“

§9 [Technische und organisatorische Maßnahmen] [1]Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. [2]Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage (zu §9 Satz 1)*

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
   - *Sicherung der Eingangsbereiche durch verschlossene Türen;*
   - *Festlegung zugangsberechtigter Personen und Ausgabe von Berechtigungsausweisen oder Schlüsseln.*
2. zu verhindern, daß Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
   - *Einführung und Durchsetzung einer wirkungsvollen Kennwortpolitik;*
   - *Chipkarten oder vergleichbare Benutzerausweise;*
   - *Erzwingen regelmäßiger Änderungen von Kennwörtern;*
   - *Abschalten von Systemen bei Erkennung unberechtigter Zugriffsversuche;*
   - *Voraussetzung ist die Zutrittskontrolle (vorstehend).*
3. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und daß personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
   - *Festlegung der jeweils erforderlichen Berechtigungen für jeden Nutzer.*
   - *Festlegung von verantwortlichen Stellen für Datenbestände und Festlegung der Genehmigung weiterer Auswertungen durch andere Stellen;*
   - *Protokollierung von Job-Aufträgen mit Programm- und Dateibenutzungen;*
   - *Verwendung elektronischer Signaturen und kryptographischer Technologien;*
   - *Voraussetzung ist die Zugangskontrolle (vorstehend).*
4. zu gewährleisten, daß personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und daß überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
   - *Verwendung elektronischer Signaturen und kryptographischer Technologien;*
   - *Festlegung von Zugriffsberechtigungen, insbesondere durch Kennwörter, Chipkarten oder dgl.;*
   - *Dokumentation des Aufrufes und der Nutzung von Clients, die der Datenübermittlung dienen;*
   - *Protokollieren aller Datenübertragungsprozesse und insbesondere der hierbei verwendeten Systemkennungen (IP-Nummern).*
5. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
   - *Maschinelle Protokollierung von Dateneingaben;*
   - *Vorgabe von Eingabe- und Prüfanweisungen;*
   - *Anweisungen über die Vergabe, Änderung, Löschung und Verwendung von Benutzerzulassungen und Passwort-Regelungen;*
   - *Differenzierung von Zugriffsberechtigungen auf Daten und Programme nach Bearbeitungsart, Modus, Dateninhalten, Zeit und ähnlichen Kriterien.*
6. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
   - *Festlegung von Regelung der Kompetenzen für Auftragserteilung und Auftragsannahme;*
   - *Festlegung von Regelung der Auftragsabwicklung.*
7. zu gewährleisten, daß personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
   - *Regelmäßige Durchführung Datensicherungen auf Medien, die nach einem anderen technischen Prinzip funktionieren (z.B. Festplatten auf optische Datenträger);*
   - *Räumliche Trennung von Datenverarbeitungsanlage und Aufbewahrung der Datensicherung;*
   - *Führung sequentieller Datensicherungen (mehrere frühere Stände);*
   - *Redundanz von Systemen (z.B. RAID-Systeme).*
8. zu gewährleisten, daß zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
   - *Sachliche und organisatorische Trennung von Datenbanken, die für unterschiedliche Zwecke erhoben und/ oder geführt werden;*
   - *Möglichkeit der Vergabe Berechtigung für einzelne Tabellen und Felder in einer Datenbank schaffen.*

* Amtlicher Text in Roman, Anmerkungen in *Italics*.

Die „Gebote für Datensicherheit und Datenschutz“

des §9 Satz 1 BDSG

1.  Zutrittskontrolle
2.  Zugangskontrolle
3.  Zugriffskontrolle
4.  Weitergabekontrolle
5.  Eingabekontrolle
6.  Auftragskontrolle
7.  Verfügbarkeitskontrolle
8.  Trennungskontrolle*

bei öffentlichen wie nichtöffentlichen Stellen, jeweils im Rahmen der Verhältnismäßigkeit.

* Nichtamtliche Bezeichnung