

## Zweck und Anwendungsbereich des BDSG

### Wie wird das Persönlichkeitsrecht durch das BDSG gesichert?

Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang mit personenbezogenen Daten. Dazu stellt es die Voraussetzungen auf, unter denen personenbezogene Daten erhoben, verarbeitet und genutzt werden dürfen. Außerdem enthält es Regeln darüber, wie mit personenbezogenen Daten umzugehen ist, damit alles fair und mit möglichst geringen Risiken abläuft. Es geht also darum, **ob** und **wie** mit personenbezogenen Daten umgegangen werden darf.

Im einzelnen lassen sich die Regelungen aufteilen in Vorschriften über:

- die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung, (s. dazu Kapitel 2, S. 16)
- die Rechte des Betroffenen, (s. dazu Kapitel 3, S. 26)
- Durchführungs- und Sicherungspflichten der Stellen, die mit personenbezogenen Daten umgehen, (s. dazu Kapitel 4, S. 37)
- die Folgen von Gesetzesverletzungen, insbesondere Strafen und Bußgeldvorschriften und (s. dazu Kapitel 4, S. 41)
- die Kontrolle des Umgangs mit personenbezogenen Daten (s. dazu Kapitel 5, S. 42)

## Welche Ziele hat der Datenschutz?

Gesetzesbestimmungen: § 1 Abs. 1 BDSG, Artikel 1 und 2 Grundgesetz

Das BDSG beginnt mit einer Umschreibung seines Zwecks:

**"Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird." (§ 1 Abs. 1 BDSG)**

Den gleichen Zweck verfolgen Datenschutzvorschriften in anderen Gesetzen.

Das Persönlichkeitsrecht gehört zu den höchsten vom Grundgesetz geschützten Werten.

**"Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt." (Artikel 1 Abs. 1 Grundgesetz)**

**"Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt." (Artikel 2 Abs. 1 Grundgesetz)**

Diese Verfassungsartikel sind auch die Grundlage des Datenschutzes.

Das Recht auf informationelle Selbstbestimmung.

Das Bundesverfassungsgericht hat dazu im Volkszählungsurteil vom 15. Dezember 1983<sup>\*)</sup> folgendes festgestellt:

**„Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.**

Zur Begründung führt das Gericht aus:

*„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermäßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“*

Das Recht auf informationelle Selbstbestimmung soll es dem einzelnen ermöglichen, sich seine Privatsphäre zu erhalten, und verhindern, daß er deshalb in zunehmende Abhängigkeit von Stellen in Staat und Wirtschaft gerät, weil diese immer mehr von ihm wissen.

Allerdings braucht der moderne Rechts- und Sozialstaat auch in großem Umfang personenbezogene Daten, um seine vielfälti-

<sup>\*)</sup> Ein Auszug aus dem Volkszählungsurteil ist als Anhang 2 abgedruckt.

gen Aufgaben fachlich richtig und gerecht erfüllen zu können. Die Schulen, die Sozialämter, die Steuerbehörden und die Polizei könnten ihre Aufgaben nicht ordentlich erfüllen, wenn sie allein auf die freiwillige Mitwirkung der Menschen angewiesen wären. Das Recht auf informationelle Selbstbestimmung kann deshalb nicht schrankenlos sein. Das hat auch das Bundesverfassungsgericht festgelegt, zugleich aber eindeutige Grenzen für Einschränkungen dieses Rechts bestimmt:

- Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur aufgrund eines Gesetzes zulässig.
- Das Gesetz muß,
- im überwiegenden Allgemeininteresse erforderlich sein,
  - die Voraussetzungen für die Einschränkung des Grundrechts und deren Umfang für den Bürger erkennbar regeln, also dem Gebot der Normenklarheit entsprechen und
  - den Grundsatz der Verhältnismäßigkeit beachten.

Wenn Gesetze in das Recht auf informationelle Selbstbestimmung des einzelnen eingreifen, dann muß der Gesetzgeber folgende Punkte beachten:

- Nur das erforderliche Minimum an Daten darf verlangt werden.
- Die Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben oder erfaßt wurden.
- Der Gesetzgeber muß durch ergänzende Vorkehrungen dafür sorgen, daß auch bei der Organisation und beim Verfahren des Umgangs mit personenbezogenen Daten auf die Rechte des einzelnen Rücksicht genommen wird (z.B. durch Mitwirkungs- und Kontrollrechte).

**Welche Begriffe sollte man kennen?**

Gesetzesbestimmung: § 3 BDSG

**Personen-  
bezogene  
Daten**.....

sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person (Betroffener), wie z.B. *Alter, Anschrift, Vermögen, Äußerungen, Überzeugungen*.

**Datei**.....

Eine **automatisierte Datei** ist eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann. Eine **nicht-automatisierte Datei** ist jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (z.B. *Stapel von Karteikarten oder Formularen*).

**Akte**.....

ist jede sonstige (nicht in Dateiform vorliegende) Unterlage, die amtlichen, dienstlichen oder geschäftsmäßigen Zwecken dient; dazu gehören auch Bild- und Tonträger (z.B. *Videoaufnahmen*), aber **nicht** Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

**Erheben**.....

ist das Beschaffen von Daten über den Betroffenen.

**Verarbeiten**.....

ist das  $\leftrightarrow$  Speichern,  $\leftrightarrow$  Verändern,  $\leftrightarrow$  Übermitteln,  $\leftrightarrow$  Sperren und  $\leftrightarrow$  Löschen von Daten.

**Nutzen**.....

ist das Verwenden von Daten, soweit nicht  $\leftrightarrow$  Verarbeiten vorliegt (z.B. *Abruf auf Bildschirm*).

**Speichern**.....

ist das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zweck ihrer weiteren  $\leftrightarrow$  Verarbeitung oder  $\leftrightarrow$  Nutzung.

**Verändern**.....

ist das inhaltliche Umgestalten gespeicherter Daten.

**Übermitteln**.....

ist das Bekanngeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen  $\leftrightarrow$  Dritten (Empfänger) in der Weise, daß

- Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
- der Empfänger bei der speichernden Stelle Daten einsieht oder abruf.

**Sperren**.....

ist das Kennzeichnen gespeicherter Daten, um ihre weitere  $\leftrightarrow$  Verarbeitung und  $\leftrightarrow$  Nutzung einzuschränken.

**Löschen**.....

ist das Unkennlichmachen gespeicherter Daten.

**Speichernde  
Stelle** .....

ist jede Person oder Stelle, die Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.

**Dritter** .....

ist jede Person oder Stelle außerhalb der  $\leftrightarrow$  speichernden Stelle;

Dritte sind nicht

- der Betroffene sowie
- Personen und Stellen, die im Inland Daten im Auftrag verarbeiten oder nutzen.

## 1 Zweck und Anwendungsbereich des BDSG

**Hinweis:** Soweit nicht ausdrücklich anders geregelt, gelten alle Begriffe sowohl für automatisierte als auch nicht-automatisierte Verarbeitung und Nutzung.

### **Achtung - Gefahr von Missverständnissen:**

Auch der Umgang mit Daten in Akten ist nach dem Gesetz „Datenverarbeitung“. Damit ist also nicht - wie in der Umgangssprache - nur Datenverarbeitung im Rahmen der Informationstechnik gemeint.

### **Welche Stellen haben das BDSG anzuwenden?**

Gesetzesbestimmungen: §§ 1 Abs. 2, 12, 27, 34 Abs 2 BDSG

Das Bundesdatenschutzgesetz gilt uneingeschränkt für öffentliche Stellen des Bundes und für nicht-öffentliche Stellen (Private). Nur sehr eingeschränkt gilt es für die öffentlichen Stellen der Länder.

Aber welche Stellen sind damit genau gemeint?

#### **Öffentliche Stellen des Bundes sind**

- Behörden des Bundes,
- Organe der Rechtspflege des Bundes,
- andere öffentlich-rechtlich organisierte Einrichtungen im Bundesbereich (z.B. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts unter Bundesaufsicht),
- bestimmte Vereinigungen öffentlicher Stellen des Bundes und bestimmte von diesen beherrschte Unternehmen, Gesellschaften oder Einrichtungen, auch in privater Rechtsform.

## Zweck und Anwendungsbereich des BDSG 1

### **Öffentliche Stellen der Länder sind**

- Behörden der Länder, Das BDSG gilt aber nur, soweit
- Organe der Rechtspflege der Länder, der Datenschutz nicht im Landesdatenschutzgesetz geregelt ist (dann gilt nur dieses) und
- andere öffentlich-rechtlich organisierte Einrichtungen im Landes- und Kommunalbereich, — diese Stellen Bundesrecht ausführen oder als Organe der Rechtspflege (ausgenommen Verwaltungsangelegenheiten) tätig werden.
- bestimmte Vereinigungen, Gesellschaften, Unternehmen und Einrichtungen öffentlicher Stellen eines Landes, auch in privater Rechtsform.

Die Länder haben jeweils ein Landesdatenschutzgesetz; nähere Informationen geben die Landesdatenschutzbeauftragten (Anschriften siehe Anhang 3).

### **Nicht-öffentliche Stellen sind**

- natürliche Personen,
  - juristische Personen des Privatrechts,
  - Personenvereinigungen des Privatrechts:
- aber nicht, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (also als "beliehene Unternehmer" tätig werden).

**Nicht-öffentliche Stellen unterliegen dem BDSG aber nur, wenn**

- personenbezogene Daten in oder aus Dateien verarbeitet oder genutzt werden (davon gibt es Ausnahmen, siehe unten auf dieser Seite) und
- die Daten geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden. Das bedeutet praktisch: Eine Verarbeitung personenbezogener Daten zu **persönlich-privaten** Zwecken unterliegt nicht dem BDSG (z.B. elektronische Notizbücher und Adressverzeichnisse sowie Aufzeichnungen im Rahmen eines Hobbies).

Das BDSG ist auch schon bei der Erhebung personenbezogener Daten zu beachten. Dies ist besonders wichtig, damit der Umgang mit den personenbezogenen Daten von Anfang an in die richtigen Bahnen gelenkt wird.

Ebenso wichtig ist, daß das BDSG auch für Daten in Akten und anderen Unterlagen (z.B. Bücher, Listen, Bildarchive, Filme, Videos, Tonaufzeichnungen) gilt. Im nicht-öffentlichen Bereich fällt generell nur die Verarbeitung und Nutzung personenbezogener Daten in oder aus einer Datei unter das Gesetz. Über diese Einschränkung hinaus gilt das BDSG nur in zwei Fällen:

- Es gilt für solche Daten, die offensichtlich aus einer Datei entnommen wurden;
- bei der Auskunft an den Betroffenen kommt es nicht auf den Dateibezug an, wenn Kreditauskunfteien (oder andere Stellen, die geschäftsmäßig personenbezogene Daten übermitteln) eine Auskunft geben.

**Welches Verhältnis besteht zwischen dem BDSG und anderen Datenschutzregelungen?**

Gesetzesbestimmung § 1 Abs. 4 BDSG

Das BDSG stellt allgemeine datenschutzrechtliche Grundregeln auf. Diese Grundregeln passen allerdings nicht überall. Und sie sind nicht überall ausreichend. Man braucht nur etwa an die Gesundheits- und Sozialbehörden, die Meldeämter, die Polizei und den Verfassungsschutz zu denken. Darum gibt es zahlreiche datenschutzrechtliche Spezialregelungen in anderen Gesetzen, wie z.B. im

- Sozialgesetzbuch,
- Straßenverkehrsgesetz,
- Melderechtsrahmengesetz,
- Ausländerzentralregistergesetz,
- Bundeszentralregistergesetz,
- Bundesverfassungsschutzgesetz,
- Bundesgrenzschutzgesetz,
- Telekommunikationsgesetz.

Diese **"bereichsspezifischen Regelungen"** gehen dem BDSG vor. Manche verschärfen den Datenschutz zugunsten des Betroffenen, andere schränken ihn auch ein.

Von großer praktischer Bedeutung für besonders schützenswerte personenbezogene Daten sind die **Berufs- und besonderen Amtsgeheimnisse**, wie z.B.

- die ärztliche Schweigepflicht,
- das Post- und Fernmeldegeheimnis,
- das Sozialgeheimnis (mehr dazu in BfD-Info 3),
- das Steuergeheimnis,
- das Personalaktengeheimnis,
- das Statistikgeheimnis,
- das Adoptionsgeheimnis.

### Zulässiger Umgang mit personenbezogenen Daten

#### Welche allgemeinen Grundsätze gelten für die Verarbeitung und Nutzung personenbezogener Daten?

Gesetzesbestimmung: § 4 BDSG

**Verarbeitung und Nutzung sind verboten...**

Für die Verarbeitung und Nutzung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Das bedeutet: Die Verarbeitung und Nutzung von Daten ist verboten, es sei denn

**es sei denn...**

— sie ist durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet oder

**eine Rechtsvorschrift oder der Betroffene erlauben sie.**

— der Betroffene hat dazu seine Einwilligung erklärt.

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen nicht an.

Soll eine Einwilligung Grundlage für eine Verarbeitung oder Nutzung sein, so ist zu beachten:

- Die Einwilligung bedarf der Schriftform (d.h. der eigenhändigen Unterschrift des Betroffenen), soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.
- Der Betroffene ist vorher über die Tragweite seiner Einwilligung aufzuklären (z.B. über den Zweck der Speicherung und eine vorgesehene Übermittlung der Daten an andere); auf Verlangen auch darüber, was geschieht, wenn er nicht einwilligt (z.B. daß dann Ansprüche verforengelassen können).

Voraussetzung für eine rechtmäßige Verarbeitung oder Nutzung personenbezogener Daten ist eine rechtmäßig einwandfreie Erhebung dieser Daten.

### Welche Regeln gelten zusätzlich für die Erhebung durch öffentliche Stellen?

Gesetzesbestimmung: § 13 BDSG

**Heimliche Datenerhebung?**

Für öffentliche Stellen ist bei der Erhebung personenbezogener Daten eine Reihe von Grundsätzen maßgeblich:

- Es dürfen nur die Daten erhoben werden, die für die Aufgabenerfüllung erforderlich sind.

**Offen und direkt beim Betroffenen.**

- Daten sind grundsätzlich beim Betroffenen zu erheben; dabei ist ihm mitzuteilen, zu welchem Zweck dies geschieht.

- Ist der Betroffene zur Auskunft verpflichtet (z.B. bei amtlichen Statistiken), so muß ihm gesagt werden, nach welchen Rechtsvorschriften das der Fall ist. Er ist auch aufzuklären, wenn er ohne die von ihm verlangten Auskünfte seine Ansprüche nicht durchsetzen kann oder ihm sonstige Rechte vorzuzusetzen entgehen.

- Andernfalls muß dem Betroffenen gesagt werden, daß die Auskunft freiwillig ist.

**Ausnahmen:**

Ohne Mitwirkung des Betroffenen (z.B. durch Anfragen bei Behörden oder anderen Stellen) dürfen Daten nur erhoben werden, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt (z.B. Einholung eines Strafregisterauszugs nach dem Bundeszentralregistergesetz) oder
- die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht (z.B. auch zur Abwehr erheblicher Gefahren durch die Polizei) und keine Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen zu erwarten ist oder

**Einige Ausnahmen gibt es...**

## 2 Zulässiger Umgang mit personenbezogenen Daten

- die Erhebung beim Betroffenen einen unverhältnismäßig hohen Aufwand zur Folge hätte (z.B. weil er sehr schwer zu finden ist) und nicht angenommen werden kann, daß seine überwiegenden schutzwürdigen Interessen dadurch beeinträchtigt werden.

Ob die befragte Stelle die erbetenen Daten übermitteln darf, muß diese aber besonders prüfen.

### **Welche Regeln gelten zusätzlich für die Speicherung, Veränderung und Nutzung durch öffentliche Stellen?**

Gesetzesbestimmung: § 14 BDSG

- Zweckentfremdung ist grundsätzlich verboten...**
- Die Speicherung, Veränderung und Nutzung personenbezogener Daten durch öffentliche Stellen ist zulässig, wenn
  - dies zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und
  - es für die Zwecke erfolgt, für die die Daten erhoben worden sind (falls keine Erhebung voranging: für die sie gespeichert worden sind). Mit der zuletzt genannten Voraussetzung wird der Zweckbindungsgrundsatz angesprochen. Von diesem sieht das Gesetz eine Reihe zum Teil weitreichender Ausnahmen vor.

### **Welche Ausnahmen von der Zweckbindung gibt es?**

- Die Verarbeitung personenbezogener Daten für einen anderen Zweck ist dann zulässig, wenn
- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
  - der Betroffene eingewilligt hat,
  - es offensichtlich im Interesse des Betroffenen liegt,
  - Angaben des Betroffenen überprüft werden müssen, weil begründete Zweifel an ihrer Richtigkeit bestehen,

aber eine Verwendung für einige andere Zwecke erlaubt das Gesetz.

## Zulässiger Umgang mit personenbezogenen Daten 2

- die Daten aus Veröffentlichungen entnommen wurden oder veröffentlicht werden dürfen (aber nicht, wenn das entgegenstehende schutzwürdige Interesse des Betroffenen offensichtlich überwiegt),

oder wenn sie

- zur Gefahrenabwehr,
- zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, oder
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte eines anderen oder
- zur Durchführung wissenschaftlicher Forschung (nach näher bestimmten Voraussetzungen)

erforderlich ist.

Auf der anderen Seite stellt das Gesetz klar, daß bestimmte Verwendungen von Daten nicht als Zweckänderung anzusehen sind, so die Verwendung für

- Hier liegt keine Zweckentfremdung vor.**
- die Rechnungsprüfung,
  - die Wahrnehmung von Aufsichts- und Kontrollbefugnissen, Organisationsuntersuchungen sowie
  - Ausbildungs- und Prüfungszwecke der speichernden Stelle, aber nur, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen (z. B. bei sehr persönlichen Angaben).

Eine strikte Zweckbindung besteht für Daten, die ausschließlich gespeichert werden zu Zwecken

- Und hier gilt die Zweckbindung strikt.**
- der Datenschutzkontrolle,
  - der Datensicherung,
  - zur Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage oder
  - der wissenschaftlichen Forschung (§ 40).

### Welche Regeln gelten zusätzlich für die Übermittlung durch öffentliche Stellen?

Gesetzesbestimmungen: §§ 15 bis 17, 39 BDSG

#### Übermittlung nach Erforderlichkeit...

- Das Gesetz kennt unterschiedliche Regelungen, je nach dem, ob eine öffentliche Stelle an
- eine andere öffentliche Stelle,
  - eine nicht-öffentliche Stelle oder
  - eine Stelle außerhalb Deutschlands
- übermittelt.

Das Übermitteln an eine öffentliche Stelle ist zulässig,

- wenn es für die Aufgabenerfüllung der übermittelnden Stelle oder des Empfängers erforderlich ist und
- der Verwendungszweck beim Empfänger gleich ist oder eine zulässige Zweckänderung vorliegt.

Werden Daten zur Erfüllung der eigenen Aufgaben an eine nicht-öffentliche Stelle übermittelt, so gelten dieselben Regelungen wie bei einer Übermittlung an eine öffentliche Stelle (siehe vorstehend).

#### oder nach Interessenabwägung.

Die Übermittlung an eine nicht-öffentliche Stelle ist außerdem zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat und der Betroffene keine schutzwürdigen Interessen am Ausschluß der Übermittlung hat. Der Betroffene muß in diesen Fällen informiert werden, außer wenn er von der Übermittlung schon auf anderem Wege weiß oder die öffentliche Sicherheit einer Unterrichtung im Wege steht.

#### Strenge Zweckbindung beim Empfänger!

Für den Empfänger gilt eine strenge Zweckbindung. Er darf die Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt wurden. Die übermittelnde Stelle muß ihm darauf ausdrücklich hinweisen. Eine Verwendung für andere Zwecke ist nur mit Zustimmung der übermittelnden Stelle erlaubt; sie kann erteilt werden, wenn die Daten auch für diesen anderen Zweck übermitteln werden dürfen.

Für die Übermittlung ins Ausland gelten die gleichen Grundsätze wie für die Übermittlung an nicht-öffentliche Stellen (siehe vorstehend). Besonderheiten können sich aus speziellen gesetzlichen Vorschriften und aus internationalen Vereinbarungen ergeben. In jedem Fall dürfen keine Daten übermittelt werden, wenn Grund zu der Annahme besteht, daß damit gegen den Zweck eines deutschen Gesetzes verstoßen würde (z.B. wenn politische Verfolgung oder Folter im Empfängerland drohen).

Auch ausländische Empfänger müssen auf die Zweckbindung hingewiesen werden. Als Empfänger im Ausland gelten auch internationale und supranationale Organisationen, z.B. die Behörden der Europäischen Gemeinschaft, auch wenn sie ihren Sitz in Deutschland haben.

### Welche Regeln gelten für die Erhebung, Verarbeitung und Nutzung zusätzlich, wenn nicht-öffentliche Stellen Daten für eigene Zwecke verwenden?

Gesetzesbestimmung: § 28 BDSG

Der größte Teil der personenbezogenen Daten der nicht-öffentlichen Stellen wird von diesen als Mittel für die Erfüllung eigener Geschäftszwecke verwendet. Dies ist z.B. der Fall bei den Daten einer Firma über Kunden, über das eigene Personal, über Lieferanten und über andere Geschäftspartner.

Für das Erheben gilt hier folgender Grundsatz:

Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.

Erhebung nach Treu und Glauben...

Praktisch bedeutet dies, daß Daten ebenso wie bei den öffentlichen Stellen grundsätzlich unter freiwilliger Mitwirkung des Betroffenen erhoben werden müssen. Heimlichkeit und Täuschung sind mit Treu und Glauben in aller Regel unvereinbar.

...ohne Heimlichkeit und Täuschung!



## 2 Zulässiger Umgang mit personenbezogenen Daten

Auch muß jede Nötigung unterbleiben. Die Datenerhebung darf auch nicht unter Umständen erfolgen, die den Betroffenen mehr als vermeidbar belasten.

In folgendem Bereich erlaubt das BDSG das Speichern, Verändern und Übermitteln:

- Im Rahmen der Zweckbestimmung eines Vertragsverhältnisses (oder vertragsähnlichen Vertrauensverhältnisses) mit dem Betroffenen (etwa zwischen Bank und Bankkunden, Arzt und Patient, Versicherung und Versicherten); entsprechend eingeschränkt auch schon vor Vertragsabschluß und nach Erledigung) oder
- soweit dies zur Wahrnehmung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß ein überwiegendes Interesse des Betroffenen entgegensteht, oder
- wenn die Daten aus allgemein zugänglichen Quellen (Telefonbüchern, Adreßbüchern, Zeitschriften usw.) entnommen werden können oder die speichernde Stelle sie veröffentlichten dürfte, aber nicht, wenn ein entgegenstehendes Interesse des Betroffenen offensichtlich überwiegt, oder
- unter bestimmten Voraussetzungen für Zwecke der wissenschaftlichen Forschung.

Die Übermittlung oder Nutzung ist außerdem in folgenden Fällen erlaubt:

- Zur Wahrung berechtigter Interessen eines Dritten oder öffentlichen Interessen, wenn kein Grund zur Annahme besteht, daß der Betroffene ein schutzwürdiges entgegenstehendes Interesse hat.

- **Am einfachsten geht's mit Adressenlisten...** Unter der letztgenannten Voraussetzung dürfen außerdem listenmäßig oder in anderer Form zusammengefaßte Daten über Angehörige einer Personengruppe übermittelt und genutzt werden.

## 2 Zulässiger Umgang mit personenbezogenen Daten

Die Daten müssen sich aber auf folgende Angaben beschränken:

- die Angabe, daß der Betroffene zu der Personengruppe gehört,
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Namen,
- akademische Grade,
- Anschrift und
- Geburtsjahr.

Eine listenmäßige Übermittlung kommt aber in der Regel nicht in Betracht,

- wenn es um die folgenden sensiblen Angaben geht:
  - gesundheitliche Verhältnisse
  - strafbare Handlungen
  - Ordnungswidrigkeiten
  - religiöse oder politische Anschauungen
  - arbeitsrechtliche Rechtsverhältnisse

*...die aber keine sensiblen Angaben enthalten dürfen.*

- und wenn diese Angaben im Zusammenhang mit einem Vertragsverhältnis (oder vertragsähnlichem Vertrauensverhältnis) gespeichert worden sind.

Diese Regelung zur listenmäßigen Übermittlung soll es ermöglichen, Daten für Zwecke der Direktwerbung oder der Markt- und Meinungsforschung bereitzustellen. Zum Ausgleich erhält der Betroffene zusätzliche Rechte. Er kann diesen Übermittlungen widersprechen und, wenn schon Daten übermittelt worden sind, beim Empfänger die Sperrung verlangen.

*Sie haben hier ein Widerspruchsrecht!*

Für den Empfänger gilt folgende Zweckbindung: Nur unter den auch für die übermittelnde Stelle geltenden Voraussetzungen darf er die erhaltenen Daten für andere Zwecke verarbeiten oder nutzen.

### **Welche Regeln gelten zusätzlich, wenn nicht-öffentliche Stellen geschäftsmäßig Daten zum Zweck der Übermittlung speichern?**

Gesetzesbestimmungen: §§ 29, 30 BDSG

Werden Daten nicht für eigene Zwecke gespeichert, sondern um sie - meist gegen Entgelt - Dritten für deren Geschäftszwecke zur Verfügung zu stellen (dies gilt vor allem für Auskunftsteilen, Kreditchutzorganisationen und Adressenhändler), so gelten folgende Grundsätze:

Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden (vgl. S. 21).

Das Speichern oder Verändern ist zulässig, wenn

- kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges entgegenstehendes Interesse hat, oder
- die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichten dürfte, außer wenn ein entgegenstehendes schutzwürdiges Interesse des Betroffenen offensichtlich überwiegt.

Das Übermitteln ist zulässig, wenn

- der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
- listenmäßig zusammengefaßte Daten (vgl. S. 23) für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen.

Außerdem darf kein Grund zur Annahme bestehen, daß der Betroffene ein schutzwürdiges entgegenstehendes Interesse hat. Bei listenmäßig zusammengefaßten Daten sind auch hier sensible Daten grundsätzlich ausgenommen. Auch in diesen Fällen hat der Betroffene ein **Widerspruchsrecht** und einen **Anspruch auf Sperrung**.

Für Markt- und Meinungsforschungsinstitute und andere Stellen, die geschäftsmäßig Daten speichern, um sie in anonymisierter Form zu übermitteln, besteht eine Verpflichtung, Namen und Adressen gesondert zu speichern. Eine Befugnis, Daten in personenbezogener Form ohne Einwilligung des Betroffenen weiterzugeben, haben sie nicht.

**Was kann man tun, wenn man durch unverlangte Werbesendungen belästigt wird?**

Die Werbewirtschaft unterhält eine Liste der Personen, die keine Werbung per Post wünschen; in diese sogenannte "Robinson-Liste" kann man sich eintragen lassen. Wer dies wünscht, erhält ein Antragsformular unter folgender Anschrift:

Deutscher Direktmarketing Verband

— Robinson-Liste —  
Postfach 14 01  
71243 Ditzingen  
Tel. 07156/951010

Die Deutsche Telekom gibt die Daten ihrer Kunden, die auf Wunsch des Kunden in das Telefonverzeichnis und ggf. in ein elektronisches Verzeichnis (z.B. CD-ROM) aufgenommen werden sollen, an die

DeTeMedien,  
Deutsche Telekom Medien GmbH  
Postfach 16 02 11  
60065 Frankfurt a. M.  
Tel.: 069/2682-0

weiter. Auch zu einem späteren Zeitpunkt kann der Kunde gegenüber der Telekom einer Eintragung widersprechen; bei der Neuaufgabe des Telefonverzeichnisses darf dann seine Anschrift nicht mehr ausgedruckt sein (Näheres zur Telekommunikation siehe BfD-Info 5).

## Rechte des Betroffenen

### Das Recht auf Auskunft

Gesetzesbestimmungen: §§ 19, 33, 34 BDSG

Jeder - unabhängig von Alter, Wohnsitz und Nationalität - hat das Recht auf Auskunft über die zu seiner Person gespeicherten Daten.

#### Welche Auskunft können Sie verlangen?

- Über die zu Ihrer Person gespeicherten Daten, einschließlich der Angabe, woher sie stammen und an welche dritten Stellen sie weitergegeben worden sind.
- über den Zweck der Speicherung (d.h. die betreffende Verwaltungsaufgabe oder den speziellen Geschäftszweck) und
- über Personen und Stellen, an die regelmäßig übermittelt wird (gilt nur bei automatisierter Verarbeitung durch nicht-öffentliche Stellen).

#### Wie erhalten Sie Auskunft?

- Gehen Sie gezielt vor!**
- Es empfiehlt sich, die Auskunft schriftlich anzufordern. Zur Legitimation genügt es in der Regel, die Kopie eines Personaldokuments beizulegen. Einschreiben ist nicht erforderlich.
  - Bei persönlicher Vorsprache wird eine sofortige Erledigung oft nicht möglich sein.
  - Wenn Sie anrufen, kann man Sie meist nicht sicher identifizieren. Deshalb gilt der Grundsatz: Keine telefonische Datenauskunft.
  - Schreiben Sie möglichst genau, worüber Sie Auskunft wünschen (also z.B. „meine Daten im Zusammenhang mit Wohngeld“ oder „im Zusammenhang mit unserem Mietvertrag“, aber nicht „alles, was die Stadtverwaltung über mich hat“).

- Wenden Sie sich an die speichernde Stelle. Wer als speichernde Stelle in Frage kommt, erfahren Sie im nachfolgenden Abschnitt „Die Rechte auf Einsicht in die Dateienregister und auf Benachrichtigung“. Außerdem können Ihnen die Datenschutzkontrollinstitutionen weiterhelfen (siehe Anhänge 3 und 4).

#### Was kostet eine Auskunft?

Grundsätzlich brauchen Sie für die Auskunft nichts zu bezahlen. Es gibt hierzu aber Ausnahmen, wie:

- Schriftliche Auskünfte von Kreditauskunfteien und ähnlichen Einrichtungen, die Sie gegenüber Dritten wirtschaftlich nutzen können (etwa um Ihre Bonität nachzuweisen). Das geforderte Entgelt darf nicht höher sein als die entstandenen direkt zu-rechenbaren Kosten. Aber auch bei derartigen Auskünften brauchen Sie dafür nichts zu bezahlen, wenn besondere Umstände dafür sprechen, daß Daten unrichtig oder unzulässig gespeichert sind oder sich dies aus der Auskunft ergibt.
- Bei einer mündlichen Auskunft oder einer Auskunft auf einem Blatt ohne Namensangabe entstehen Ihnen keine Kosten. Auf die Möglichkeit, durch persönliche Kenntnisnahme die Auskunft unentgeltlich zu erhalten, muß die speichernde Stelle Sie ausdrücklich hinweisen.

#### Was ist an Besonderheiten zu beachten?

##### Bei öffentlichen Stellen

- Über personenbezogene Daten in Akten erhalten Sie nur Auskunft, wenn

### 3 Rechte des Betroffenen

*Für eine Auskunft aus Akten müssen Sie mit-  
helfen.*

- Sie Angaben machen, die das Auffinden der Daten ermöglichen, und
- der Arbeitsaufwand nicht außer Verhältnis zu Ihrem Informationsinteresse steht. Legen Sie deshalb dar, warum Ihnen die Auskunft wichtig ist.

- Eine Auskunft darüber, ob Daten an einen Nachrichtendienst (Bundesamt für Verfassungsschutz, Militärischer Abschirmdienst und Bundesnachrichtendienst) übermittelt wurden, ist nur mit dessen Zustimmung zugelassen.

#### **Bei nicht-öffentlichen Stellen**

- Von Kreditauskunfteien und anderen Stellen, die geschäftsmäßig Daten zum Zweck der Übermittlung speichern, können Sie Auskunft auch über Daten verlangen, die nicht in einer Datei gespeichert sind (z.B. in Akten oder Heften).
- Diese Stellen müssen Ihnen auch sagen, woher sie Ihre Daten haben und wohin diese übermittelt worden sind, wenn Sie begründete Zweifel an der Richtigkeit der Daten geltend machen können.

#### **In welchen Fällen hat man keinen Anspruch auf Auskunft?**

**Öffentliche Stellen** verweigern die Auskunft, soweit

- *Nicht immer gibt es eine Auskunft.* sonst die Gefahr besteht, daß sie ihre Aufgabe nicht ordnungsgemäß erfüllen können, z.B. wenn laufende polizeiliche Ermittlungen gefährdet würden,
- es notwendig ist zum Schutz der öffentlichen Sicherheit oder Ordnung (kommt nur selten vor) oder
- die Daten oder die Tatsache, daß die Stelle sie speichert, geheim gehalten werden müssen (aus gesetzlichen Gründen oder im Geheimhaltungsinteresse eines Dritten, z.B. Adoptionsgeheimnis; im übrigen sehr selten), und deswegen

### 3 Rechte des Betroffenen

das Interesse des Betroffenen an der Auskunft zurücktreten muß. Die Auskunft darf aber nie pauschal abgelehnt werden, sondern nur nach sorgfältiger Abwägung im Einzelfall.

**Nicht-öffentliche Stellen** dürfen eine Auskunft nur in Fällen ablehnen, in denen auch keine Benachrichtigungspflicht besteht (Einzelheiten in § 34 Abs. 4 in Verbindung mit § 33 Abs. 2 Nr. 2 bis 6).

#### **Was tun, wenn die Auskunft verweigert wird?**

Sie haben grundsätzlich Anspruch auf eine vollständige Auskunft, d.h. alle Angaben, für die nach dem Gesetz grundsätzlich eine Auskunftsverpflichtung besteht, müssen Ihnen mitgeteilt werden.

Soweit die auskunftspflichtige Stelle von einer der oben beschriebenen gesetzlichen Möglichkeiten Gebrauch macht und nur teilweise Auskunft erteilt, muß sie auf die Unvollständigkeit der Auskunft ausdrücklich hinweisen, damit Sie die Möglichkeit haben, eine Überprüfung zu verlangen.

Im allgemeinen ist die auskunfterteilende Stelle auch verpflichtet zu begründen, aufgrund welcher gesetzlichen Bestimmung und aufgrund welcher Tatsachen sie eine Auskunft über bestimmte Punkte ablehnt. Eine solche Begründung ist nur erbehrlich, wenn sonst der mit der Auskunftsverweigerung verfolgte Zweck (z.B. laufende polizeiliche Ermittlungen nicht zu behindern) gefährdet würde.

*Der BfD kann helfen.*

Haben Sie Zweifel, ob Ihnen korrekt Auskunft erteilt worden ist, können Sie sich an den Bundesbeauftragten für den Datenschutz oder an die sonst zuständige Datenschutzkontrollinstitution wenden. Fügen Sie Ihren Schriftwechsel in Kopie bei. Ihr Vorgang wird dann umfassend überprüft, und Sie erhalten in jedem Fall Bescheid, ob Ihre Rechte beachtet wurden. Sie haben außerdem die Möglichkeit einer gerichtlichen Klage.

#### Die Rechte auf Einsicht in die Dateienregister und auf Benachrichtigung

Gesetzesbestimmungen: §§ 26 Abs. 5, 32, 33, 38 Abs. 2 BDSG

##### Die Registereinsicht

Die Behörden und öffentlichen Stellen des Bundes haben ihre automatisierten Dateien, in denen personenbezogene Daten gespeichert werden, dem Bundesbeauftragten für den Datenschutz zur Aufnahme in ein Register zu melden. Dieses Register kann von jedermann eingesehen werden. Der Registerinhaber kann Ihnen Anhaltspunkte geben, bei welchen Stellen Sie Ihr Auskunftsrecht ausüben möchten.

Zu jeder automatisierten Datei enthält das Register folgende Angaben:

1. Bezeichnung und Art der Datei,
2. Zweckbestimmung,
3. Art der gespeicherten Daten,
4. betroffener Personenkreis,
5. Art der regelmäßig zu übermittelnden Daten und deren Empfänger,
6. Regelfristen für die Datenlöschung.

**Hinweis:** Aus dem Register kann also nicht entnommen werden, ob überhaupt und, wenn ja, welche Daten gerade über Sie oder eine andere Einzelperson wo gespeichert sind.

##### Ausnahmen:

Nicht in das Register aufgenommen werden

- die Dateien folgender Behörden:
  - Verfassungsschutzbehörden,
  - Bundesnachrichtendienst,
  - Militärischer Abschirmdienst,
  - andere Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird.

- vorübergehend angelegte Dateien, die spätestens drei Monate nach ihrer Erstellung gelöscht werden.

Bei Dateien der Staatsanwaltschaft und der Polizei sowie bei bestimmten Stellen der Finanzverwaltung unterliegen folgende Angaben nicht der öffentlichen Einsicht:

- Art der gespeicherten Daten,
- Art der regelmäßig zu übermittelnden Daten und deren Empfänger.

Im nicht-öffentlichen Bereich gibt es nur für einen relativ kleinen Teil der Dateien ein öffentliches Dateienregister, nämlich für die nicht-öffentlichen Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (auch in anonymisierter Form) speichern oder sie im Auftrag als Dienstleistungsentnehmen verarbeiten oder nutzen. Hierunter fallen vor allem Kreditankunftsstellen, Markt- und Meinungsforschungsinstitute und Dienstleistungsrechenzentren. Diese Stellen haben der zuständigen Aufsichtsbehörde (siehe Anhang 4) innerhalb eines Monats die Aufnahme, Änderungen und die Beendigung ihrer Tätigkeit zu melden und dabei folgende Angaben zum öffentlichen Register mitzuteilen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer und sonstige Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift,
4. Geschäftszwecke der Stelle und der Datenverarbeitung,
5. Name des von der Stelle Beauftragten für den Datenschutz,
6. allgemeine Beschreibung der Art der gespeicherten personenbezogenen Daten (nicht bei im Auftrag verarbeiteten oder genutzten Daten).

**Die Benachrichtigung**

Ein anderes wichtiges Mittel, damit Sie wissen (können), wer welche Daten über Sie verarbeitet, ist im **nicht-öffentlichen Bereich** die Benachrichtigung.

**Wann werden Sie benachrichtigt?** Jede nicht-öffentliche Stelle ist verpflichtet, alle Betroffenen individuell zu benachrichtigen, über die sie Daten ohne deren Kenntnis verarbeitet.

Der Zeitpunkt der Benachrichtigung ist unterschiedlich. Stellen, die personenbezogene Daten für eigene Zwecke verarbeiten, benachrichtigen zum Zeitpunkt der ersten Speicherung. Die (vorstehend genannten) Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung speichern, benachrichtigen erst zum Zeitpunkt der erstmaligen Übermittlung.

Die Benachrichtigung muß umfassen:

- Angabe der speichernden Stelle mit Name/Firma und Anschrift,
- die Tatsache, daß erstmals Daten über die Person, die benachrichtigt wird, gespeichert oder übermittelt werden, und
- die Art der Daten.

In bestimmten im Gesetz genannten Fällen erfolgt keine Benachrichtigung, etwa weil eine überwiegende Geheimhaltungspflicht besteht oder weil die Datenverarbeitung nach Auffassung des Gesetzgebers für den Betroffenen weniger gravierend ist. Vergleiche im einzelnen § 33 Abs. 2.

**Ausnahmen!**

**Die Rechte auf Berichtigung, Sperrung oder Löschung**

Gesetzesbestimmungen: §§ 20, 35 BDSG

**Wann sind personenbezogene Daten zu berichtigen?**

Jede Stelle ist verpflichtet, unrichtige Daten zu berichtigen. Es liegt aber auch am Betroffenen selbst, darauf hinzuweisen, wenn Daten unrichtig oder überholt sind.

In Akten werden unrichtige Daten nicht durch richtige ausgetauscht, es wird aber ein Berichtigungsvermerk beigefügt. Ebenso ist zu vermerken, wenn der Betroffene die Richtigkeit bestreitet.

**Wann sind personenbezogene Daten zu löschen?**

- Von öffentlichen Stellen, wenn
- ihre Speicherung unzulässig ist, etwa weil schon die Erhebung unzulässig war, oder
  - die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist.
- Daten, die man nicht haben dürfte oder nicht mehr braucht, sind zu löschen.

Von nicht-öffentlichen Stellen, wenn

- die Speicherung unzulässig ist, etwa weil schon die Erhebung unzulässig war, oder
- es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und die speichernde Stelle deren Richtigkeit nicht beweisen kann, oder
- für eigene Zwecke verarbeitete Daten für die Erfüllung des Speicherungszwecks nicht mehr erforderlich sind, oder
- geschäftsmäßig zum Zweck der Übermittlung verarbeitete Daten aufgrund einer am Ende des fünften Kalenderjahres nach der ersten Speicherung vorzunehmenden Prüfung nicht mehr erforderlich sind (z.B. bei Auskunfteien und Adressverlagen).

#### Achtung!

Eine Löschung ist nur für personenbezogene Daten vorgesehen, die in einer Datei verarbeitet werden, jedoch nicht für einzelne Daten, die in Akten festgehalten sind. Sind allerdings komplette Akten unzulässig angelegt, so sind sie ebenfalls zu vernichten; ebenso ist im allgemeinen mit nicht mehr erforderlichen Akten zu verfahren.

#### Wann sind personenbezogene Daten zu sperren?

Personenbezogene Daten sind immer dann zu sperren, wenn einer fälligen Löschung besondere Gründe entgegenstehen, etwa

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen, etwa weil ihm Beweismittel verlorengehen, oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Personenbezogene Daten sind zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

Öffentliche Stellen haben personenbezogene Daten in Akten zu sperren, wenn sie im Einzelfall feststellen, daß sonst schutzwürdige Interessen des Betroffenen beeinträchtigt würden, und sie die Daten nicht mehr zur Aufgabenerfüllung benötigen.

Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn dies

- zu wissenschaftlichen Zwecken,
- zur Behebung einer bestehenden Beweisnot oder
- aus sonstigen im überwiegenden Interesse der sichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist.

#### Das Recht auf Anrufung des Bundesbeauftragten für den Datenschutz und anderer Kontrollinstitutionen

Gesetzesbestimmungen: §§ 21, 38 BDSG

Wer annimmt, bei der Erhebung, Verarbeitung oder Nutzung seiner persönlichen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein, kann sich an den Bundesbeauftragten für den Datenschutz wenden. Als unabhängige Beschwerdeinstanz mit umfassenden Kontrollbefugnissen (mehr im Kapitel 5) geht der Bundesbeauftragte allen Eingaben nach und unterrichtet den Betroffenen vom Ergebnis.

Alle Eingaben werden vertraulich behandelt. Auf Wunsch des Betroffenen bleibt sein Name auch gegenüber der öffentlichen Stelle ungenannt, über die er sich beschwert.

Entsprechend können Sie den jeweiligen Landesbeauftragten für den Datenschutz anrufen, wenn Sie Ihre Rechte durch eine öffentliche Stelle eines Landes verletzt sehen.

Wer meint, durch den Umgang mit seinen Daten seitens einer nicht-öffentlichen Stelle in seinen Rechten verletzt zu sein, kann sich an die Aufsichtsbehörde des jeweiligen Landes wenden. Die örtliche Zuständigkeit richtet sich nach dem Sitz der nicht-öffentlichen Stelle.

Anschriften und Telefonnummern der Datenschutzkontrollinstitutionen finden Sie in den Anhängen 3 und 4.

#### Das Recht auf Schadensersatz

Gesetzesbestimmungen: §§ 7, 8 BDSG

Durch eine über die Haftung nach dem Bürgerlichen Gesetzbuch hinausgehende Verpflichtung zum Schadensersatz bei unrichtiger oder unzulässiger automatisierter Datenverarbeitung verbessert das Gesetz den Schutz des Persönlichkeitsrechts, auch indem es auf diese Weise die datenverarbeitenden Stellen zu besonderer Sorgfalt beim Umgang mit personenbezogenen Daten anhält.

#### Schadensersatzanspruch gegen eine öffentliche Stelle

Öffentliche Stellen haften nach dem Prinzip der Gefährdungshaftung, d.h. sie sind unabhängig von einem Verschulden zum Ersatz des Schadens verpflichtet (bis höchstens 250.000 DM).

**Gefährdungshaftung!**

Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen auch der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen (Schmerzensgeld).

**Schmerzensgeld!**

#### Schadensersatzanspruch gegen eine nicht-öffentliche Stelle

Bei der Geltendmachung eines Schadensersatzanspruchs gegenüber einer nicht-öffentlichen Stelle hilft das Gesetz dem Geschädigten durch eine Beweislastumkehr. Ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so muß sie beweisen, daß das nicht der Fall ist. Kann sie das nicht, so haftet sie.

**Beweislastumkehr!**

## Praxis des Datenschutzes

### Die Durchführung des Datenschutzes bei öffentlichen Stellen

Gesetzesbestimmung: § 18 BDSG

**Jede Stelle muß sich Übersicht verschaffen.**

Das Gesetz verlangt, daß jede öffentliche Stelle sich über die für den Datenschutz wichtigen Sachverhalte eine präzise Informationsgrundlage schafft und diese auf dem jeweils neuesten Stand hält. So muß für jede Datei eine Reihe von Punkten schriftlich festgelegt werden. Es handelt sich dabei um dieselben Angaben, die auch zum öffentlichen Datenregister zu melden sind (s. dazu S. 30).

Außerdem ist ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen zu führen.

Diese Informationsgrundlagen sind notwendig, damit systematisch geprüft werden kann, ob der Umgang mit personenbezogenen Daten den datenschutzrechtlichen Anforderungen entspricht und ob alles getan wurde, damit die Daten im gesamten Geschäftsablauf richtig geschützt sind. Sie sind das wichtigste Arbeitsmittel derjenigen, die innerhalb der öffentlichen Stellen dafür zu sorgen haben, daß der Datenschutz funktioniert. Wer das sein soll, sagt das Gesetz nicht. Es hat sich aber in der Praxis weitgehend eingebürgert, daß die Behördenleiter einen Mitarbeiter (behördlichen Datenschutzbeauftragten) oder ein bestimmtes Referat mit allen zentralen Aufgaben des Datenschutzes betrauen. Diese Stelle ist dann Ansprechpartner für Betroffene und auch für Kontakte mit dem Bundesbeauftragten für den Datenschutz zuständig.

Auch die vom Gesetz geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme kann dieser Person oder Organisationseinheit übertragen werden, ggf. in Zusammenarbeit mit einem Mitarbeiter aus dem Bereich der automatisierten Datenverarbeitung.



### Die Durchführung des Datenschutzes bei nicht-öffentlichen Stellen

Gesetzesbestimmungen: §§ 36, 37 BDSG

**Der firmeninterne Datenschutzbeauftragte ist eine wichtige Person mit vielen Aufgaben.**

Im nicht-öffentlichen Bereich steht der Beauftragte für den Datenschutz im Mittelpunkt der gesetzlichen Regelung. Von einer gewissen Größe ab hat jede nicht-öffentliche Stelle einen Beauftragten für den Datenschutz zu berufen und ihn unmittelbar der Leitung zu unterstellen. Er muß die erforderliche Fachkunde und Zuverlässigkeit aufweisen und ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

Seine Aufgabe ist es, die Ausführung des BDSG und anderer Datenschutzvorschriften umfassend sicherzustellen. Schwerpunkte seiner Tätigkeit sind:

- Prüfung der Zulässigkeit des Umgangs mit Daten,
- Überwachung der ordnungsgemäßen Programmanwendung,
- Unterrichtung von Mitarbeitern über die Anforderungen des Datenschutzes.

Als wichtiges Arbeitsmittel hat ihm die nicht-öffentliche Stelle eigene Datenübersicht und eine Übersicht der eingesetzten Datenverarbeitungsanlagen zur Verfügung zu stellen und ihn auch sonst bei der Erfüllung seiner Aufgaben zu unterstützen.

Der Beauftragte für den Datenschutz kann sich in Zweifelsfällen an die Aufsichtsbehörde wenden. In bezug auf personenbezogene Daten ist er zur Verschwiegenheit verpflichtet, soweit der Betroffene ihn nicht davon befreit. Zu seinem eigenen Schutz bestimmt das Gesetz, daß er nicht benachteiligt werden darf. Seine Bestellung kann nur unter erschwerten Bedingungen widerrufen werden.

### Technische und organisatorische Maßnahmen

Gesetzesbestimmungen: §§ 9, 10 BDSG

Ein sehr wichtiger, oft arbeits- und kostenintensiver Bereich des Datenschutzes sind die technischen und organisatorischen Maßnahmen, die getroffen werden müssen, damit die personenbezogenen Daten vor Mißbrauch, Fehlern und Unglücksfällen möglichst sicher sind. Welche Maßnahmen notwendig sind, hängt nicht nur von der Art der Daten ab, sondern ebenso von der Aufgabe, den organisatorischen Bedingungen, den räumlichen Verhältnissen, der personellen Situation und anderen Rahmenbedingungen. Das Gesetz verzichtet deshalb darauf, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, sondern verlangt nur allgemein,

"die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes ... zu gewährleisten."

Welche Wirkung diese Maßnahmen im Bereich der automatisierten Verarbeitung haben müssen, legt das Gesetz in Form einer Anlage zu § 9\*) katalogmäßig fest. Die Maßnahmen müssen beispielsweise geeignet sein,

- Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren,
- zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können und daß eine unbefugte Dateneingabe möglich ist, und
- die behördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.

\*) Der volle Text der Anlage ist am Ende des Gesetzes abgedruckt.

**Die technische-organisatorische Umsetzung verlangt ein abgestimmtes Konzept.**

Bei den technischen und organisatorischen Maßnahmen ist von entscheidender Bedeutung, daß sie als ein zusammenwirkendes Schutzsystem verstanden werden. Viele Maßnahmen des Datenschutzes wirken zugleich im Sinne einer Sicherung eines ordentlichen Betriebsablaufs. Deshalb ist es wichtig, das Datenschutzkonzept jeweils in engem Zusammenhang mit sonstigen Sicherheitskonzepten zu entwickeln und anzuwenden.

Während das Gesetz allgemein in bezug auf technische Fragen eher zurückhaltend ist, stellt es für die Einrichtung eines **automatisierten Verfahrens zum Abruf personenbezogener Daten** durch Dritte genaue Anforderungen auf, weil es darin eine besonders einschneidende Maßnahme sieht.

Damit die Zulässigkeit des Abrufverfahrens kontrolliert werden kann, müssen die beteiligten Stellen folgendes schriftlich festlegen:

- Anlaß und Zweck des Abrufverfahrens,
- Datenempfänger,
- Art der zu übermittelnden Daten,
- nach § 9 erforderliche technische und organisatorische Maßnahmen.

Die Einrichtung des automatisierten Abrufverfahrens ist nur zulässig, wenn es unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen einerseits und der Aufgaben oder Geschäftszwecke der beteiligten Stellen andererseits angemessen ist.

### **Straf- und Bußgeldvorschriften**

Gesetzesbestimmungen: §§ 43, 44 BDSG

Verstöße gegen die wichtigsten Vorschriften zur Zulässigkeit der Datenverarbeitung werden als Straftat verfolgt und mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe belegt. Auch das Erschleichen von Daten durch unrichtige Angaben und die Zweckentfremdung sowie bestimmte Fälle der Datenverknüpfung sind unter Strafe gestellt.

*Sie müssen tätig werden!*

Die Staatsanwaltschaft wird nur auf Antrag tätig. Nur der durch den Datenschutzverstoß Betroffene kann den Strafantrag stellen.

Die Bußgeldvorschriften greifen im wesentlichen ein, wenn nicht-öffentliche Stellen ihren Meldepflichten, ihrer Pflicht zur Benachrichtigung eines Betroffenen oder ihrer Pflicht zur Bestellung eines Beauftragten für den Datenschutz nicht oder nicht ordnungsgemäß nachkommen.

Ebenso wie die Schadensersatzvorschriften haben die Straf- und Bußgeldvorschriften eine wichtige präventive Funktion.

## Kontrolle des Datenschutzes

### Notwendigkeit der Datenschutzkontrolle

Mit Hilfe Ihrer Rechte nach dem BDSG können Sie feststellen, welche Stellen welche Angaben zu Ihrer Person verarbeiten und nutzen, und Sie können ggf. Korrekturen verlangen. Außerdem wurden in Bund und Ländern - und ähnlich in den meisten demokratischen Staaten - besondere Kontrollinstitutionen eingerichtet, die dafür sorgen sollen, daß der Datenschutz auch in der Praxis wirkungsvoll umgesetzt wird. Dafür gibt es verschiedene Gründe:

- Die Kontrolle durch den einzelnen ist begrenzt. Besonders bei den Sicherheitsbehörden steht oft die Geheimhaltung einer vollen Information der Betroffenen entgegen. Hier kann ein unabhängiges Kontrollorgan die Kontrolle stellvertretend ausüben und dem Betroffenen die Sicherheit geben, daß seine Rechte nicht vernachlässigt werden.
- Bei der Komplexität der behördlichen und technischen Abläufe braucht der einzelne oft einen fachkundigen Anwalt, der ihm den "Durchblick" verschafft und seiner Sache den notwendigen Nachdruck verleiht.
- Der Bundestag hat mit dem Bundesbeauftragten für den Datenschutz eine Institution geschaffen, die ihn unparteiisch und fachkundig über alle Entwicklungen auf dem Gebiet des Datenschutzes unterrichtet und ihm Hinweise gibt, wo er durch Gesetze oder andere Maßnahmen in die Entwicklung eingreifen sollte.
- Auch der Bundesregierung und den Behörden des Bundes steht der Bundesbeauftragte für den Datenschutz als fachkundiger Berater beim Lösen von Datenschutzproblemen zur Seite.
- Vor allem aber soll der Bundesbeauftragte durch die Kontrolle aller öffentlicher Stellen des Bundes sicherstellen, daß das Recht auf Datenschutz nicht nur auf dem Papier steht.

### Der Bundesbeauftragte für den Datenschutz

Gesetzesbestimmungen: §§ 22 bis 26 BDSG

Der Bundesbeauftragte für den Datenschutz wird vom Deutschen Bundestag für eine Amtszeit von fünf Jahren gewählt. Er ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Dies bedeutet z.B., daß weder einzelne Minister noch die Bundesregierung im ganzen ihm Weisungen in bezug auf seine Amtstätigkeit geben können.

Die Dienststelle des Bundesbeauftragten umfaßt 53 Mitarbeiter. Sie ist in sieben Referate untergliedert, die u. a. folgende Zuständigkeiten haben (Stand 1996):

- I Grundsatzangelegenheiten, Internationales, nicht-öffentlicher Bereich, Meldewesen
- II Rechtswesen, Finanzen, Arbeitsverwaltung, Verteidigung, Zivildienst, Auswärtiger Dienst
- III Sozialwesen (Renten-, Kranken-, Unfall- und Pflegeversicherung), Personalwesen
- IV Wirtschaft und Verkehr, Multimedia, Forschung, Statistik, Archivwesen, Gesundheitswesen, Post, Umweltangelegenheiten
- V Polizei, Nachrichtendienste, Sicherheitsüberprüfung
- VI Informationstechnik, Telekommunikation, Datensicherung
- VII Allgemeine innere Verwaltung, Strafrecht, Aufarbeitung der MfS-Unterlagen

### Die Aufgaben des Bundesbeauftragten für den Datenschutz

Der Bundesbeauftragte hat drei Hauptaufgaben:

- die Bearbeitung von Eingaben (vgl. dazu S. 35).
- die Kontrolle und
- die Beratung.

Der Bundesbeauftragte kontrolliert alle öffentlichen Stellen des Bundes von den Dienststellen des Zolls, des Grenzschutzes, der Bundeswehr über die Wasser- und Schifffahrtsdirektionen bis hin zu den Trägern der sozialen Sicherung, z. B. die Arbeitsämter, die Betriebskrankenkassen oder die Ersatzkassen, und den Nachrichtendiensten. Jedes Jahr werden etwa 30 Behörden in einer mehrtägigen Kontrolle umfassend oder in bestimmten Ausschnitten daraufhin überprüft, ob der Datenschutz korrekt eingehalten wird. Dabei geht es nicht nur um das Bundesdatenschutzgesetz und die bereichsspezifischen Rechtsvorschriften, sondern z. B. auch um die Gestaltung von Fragebögen, die Sicherheit in Netzen oder die datenschutzgerechte Altpapiersorgung. Kontrolliert wird aber auch, ob z. B. Auskunftswünsche von Betroffenen richtig erfüllt worden sind und ob bei Datenübermittlungen an andere Stellen nicht zu großzügig verfahren wird. Die Kontrollergebnisse werden in einem schriftlichen Kontrollbericht niedergelegt.

Ebenso wichtig wie die Kontrolle ist die Beratung. Der Bundesbeauftragte berät

- die Behörden und öffentlichen Stellen des Bundes (einschließlich ihrer Personalvertretungen) bei allen Fragen, die mit der praktischen Umsetzung des Datenschutzes verbunden sind,
- die Ministerien (auch bei der Vorbereitung von Gesetzen und Vorschriften über den Datenschutz),
- den Bundestag und die Bundesregierung durch Erstattung von Gutachten, die diese anfordern können, und
- die Ausschüsse des Bundestages bei Gesetzesberatungen, bei der Beratung seiner Tätigkeitsberichte und aus anderen Anlässen.

### Die Befugnisse des Bundesbeauftragten für den Datenschutz

Der Bundesbeauftragte hat umfassende Untersuchungsbefugnisse. Alle öffentlichen Stellen des Bundes sind verpflichtet, ihn und seine Mitarbeiter bei der Erfüllung ihrer Aufgaben zu unterstützen. Insbesondere müssen sie

- seine Fragen beantworten,
- ihm Einsicht in alle Unterlagen und Akten gewähren, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, und
- ihm jederzeit Zutritt zu allen Diensträumen gestatten.

Der Bundesbeauftragte hat auch Zugang zu Unterlagen, die einer besonderen Geheimhaltung unterliegen (vgl. dazu § 24 Abs. 2). Den Umgang mit personenbezogenen Daten, die nur in Akten gespeichert sind (also nicht in Dateien), kontrolliert der Bundesbeauftragte nur, wenn Anhaltspunkte für Datenschutzverstöße bestehen, etwa aufgrund der Eingabe eines Betroffenen.

Stellt der Bundesbeauftragte Datenschutzverstöße fest, so beanstandet er sie förmlich. Darauf kann er aber verzichten, wenn die Mängel unerheblich sind oder inzwischen beseitigt wurden. Im Falle einer Beanstandung muß sich das zuständige Ministerium oder die sonstige höchste vorgesezte Stelle um die Angelegenheit kümmern. Sie wird dann auch prüfen müssen, ob Anlaß besteht, über den Einzelfall hinaus korrigierende Maßnahmen zu treffen.

Der Bundesbeauftragte behandelt wichtige Fälle, vor allem An gelegenheiten, die aus der Sicht des Datenschutzes nicht befriedigend gelöst wurden, in seinem **Tätigkeitsbericht**<sup>\*)</sup>, den er alle zwei Jahre dem Bundestag erstattet. Die Tätigkeitsberichte finden beim Bundestag große Beachtung. Sie werden in den zuständigen Ausschüssen beraten. In vielen Fällen hat der Bundestag Anregungen aufgegriffen, etwa

<sup>\*)</sup> Der Tätigkeitsbericht kann beim Bundesbeauftragten kostenlos angefordert werden.

- durch die Aufforderung an die Bundesregierung, den Bundesbeauftragten bei allen datenschutzrelevanten Vorhaben, insbesondere bei Gesetzgebungsvorhaben, frühzeitig zu beteiligen,
- durch die Aufforderung an die Bundesregierung, zu bestimmten Fragen Gesetzentwürfe vorzubereiten, oder
- durch die Aufforderungen an die Bundesregierung, die Verwaltungspraxis in bestimmten Punkten datenschutzfreundlicher zu gestalten oder über bestimmte Problembereiche gesondert Bericht zu erstatten.

### **Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich**

Gesetzesbestimmung: § 38 BDSG

Für die Kontrolle des Datenschutzes bei den nicht-öffentlichen Stellen sind die Aufsichtsbehörden der Länder zuständig, die von den Landesregierungen zu bestimmen sind. Meist sind dies die Innenminister oder -senatoren oder die Mittelbehörden (Regierungspräsidenten, Bezirksregierungen). In manchen Ländern ist der Landesbeauftragte für den Datenschutz zugleich Aufsichtsbehörde.

Die Aufsichtsbehörde überprüft ebenfalls die Ausführung des BDSG und anderer Vorschriften über den Datenschutz, im allgemeinen allerdings nur

- soweit es um die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien geht und
- wenn Anhaltspunkte für einen Datenschutzverstoß vorliegen, etwa wenn ein Betroffener dies begründet darlegt.

Nur in einem Teilbereich wird die Aufsichtsbehörde auch ohne besonderen Anlaß tätig, nämlich soweit es sich um die geschäftsmäßige Speicherung zum Zweck der (auch anonymisier-

ten) Übermittlung handelt oder wenn Daten im Auftrag durch Dienstleistungsunternehmen verarbeitet werden. Dies ist der Bereich, der auch zum Dateiregister der Aufsichtsbehörde zu melden ist (siehe S. 31).

Auch die Aufsichtsbehörde hat das Recht, Grundstücke und Geschäftsräume der zu prüfenden Stelle zu betreten, dort Prüfungen und Besichtigungen vorzunehmen und geschäftliche Unterlagen einzusehen. Vor allem aber haben die überprüften Stellen und deren Leitungspersonal der Aufsichtsbehörde auf Verlangen alle erforderlichen Auskünfte unverzüglich zu erteilen. Die Aufsichtsbehörde muß sie aber darauf hinweisen, daß sie die Auskunft auf Fragen verweigern können, deren Beantwortung sie oder ihre Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens wegen einer Ordnungswidrigkeit aussetzen würde.

Stellt die Aufsichtsbehörde technische oder organisatorische Mängel fest, so kann sie Maßnahmen zur Abhilfe anordnen. Bei schwerwiegenden Mängeln mit besonderer Gefährdung des Persönlichkeitsrechts kann sie auch den Einsatz einzelner Verfahren untersagen. Sie kann auch verlangen, daß ein Beauftragter für den Datenschutz abberufen wird, wenn es ihm an Fachkunde oder Zuverlässigkeit fehlt. Daneben können Maßnahmen nach der Gewerbeordnung ergriffen werden.

## Bundesdatenschutzgesetz (BDSG)

vom 20. Dezember 1990<sup>\*)</sup> (BGBl. I S. 2954)

### Erster Abschnitt

#### Allgemeine Bestimmungen

- § 1 Zweck und Anwendungsbereich des Gesetzes
- § 2 Öffentliche und nicht-öffentliche Stellen
- § 3 Weitere Begriffsbestimmungen
- § 4 Zulässigkeit der Datenverarbeitung und -nutzung
- § 5 Datengeheimnis
- § 6 Unabhängbare Rechte des Betroffenen
- § 7 Schadensersatz durch öffentliche Stellen
- § 8 Schadensersatz durch nicht-öffentliche Stellen
- § 9 Technische und organisatorische Maßnahmen
- § 10 Einrichtung automatisierter Abrufverfahren
- § 11 Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

### Zweiter Abschnitt

#### Datenverarbeitung der öffentlichen Stellen

#### Erster Unterabschnitt

#### Rechtsgrundlagen der Datenverarbeitung

- § 12 Anwendungsbereich
- § 13 Datenerhebung

- § 14 Datenspeicherung, -veränderung und -nutzung
- § 15 Datenübermittlung an öffentliche Stellen
- § 16 Datenübermittlung an nicht-öffentliche Stellen
- § 17 Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes
- § 18 Durchführung des Datenschutzes in der Bundesverwaltung

### Zweiter Unterabschnitt

#### Rechte des Betroffenen

- § 19 Auskunft an den Betroffenen
- § 20 Berichtigung, Löschung und Sperrung von Daten
- § 21 Anrufung des Bundesbeauftragten für den Datenschutz

### Dritter Unterabschnitt

#### Bundesbeauftragter für den Datenschutz

- § 22 Wahl des Bundesbeauftragten für den Datenschutz
- § 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz
- § 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz
- § 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz
- § 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz; Dateiregister

### Dritter Abschnitt

#### Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

#### Erster Unterabschnitt

#### Rechtsgrundlagen der Datenverarbeitung

- § 27 Anwendungsbereich
- § 28 Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke
- § 29 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung
- § 30 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form
- § 31 Besondere Zweckbindung
- § 32 Meldepflichten

### Zweiter Unterabschnitt

#### Rechte des Betroffenen

- § 33 Benachrichtigung des Betroffenen
- § 34 Auskunft an den Betroffenen
- § 35 Berichtigung, Löschung und Sperrung von Daten

### Dritter Unterabschnitt

#### Beauftragter für den Datenschutz, Aufsichtsbehörde

- § 36 Bestellung eines Beauftragten für den Datenschutz
- § 37 Aufgaben des Beauftragten für den Datenschutz
- § 38 Aufsichtsbehörde

### Vierter Abschnitt

#### Sondervorschriften

- § 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs oder besonderen Amtsgeheimnis unterliegen
- § 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen
- § 41 Verarbeitung und Nutzung personenbezogener Daten durch die Medien
- § 42 Datenschutzbeauftragte der Rundfunkanstalten des Bundesrechts

### Fünfter Abschnitt

#### Schlussvorschriften

- § 43 Strafvorschriften
- § 44 Bußgeldvorschriften

Anlage zu § 9 Satz 1

<sup>\*)</sup> Stand: August 1995