

Vorlesung: Grundlagen des Datenschutzrechts

1. Einleitung

a) Arbeitsmaterialien/Literatur: Unbedingt erforderlich sind die Texte des **Bundesdatenschutzgesetzes**, des **Telekommunikationsgesetzes** und des **Teledienste-Datenschutzgesetzes**. Hilfreich ist auch der Text des Grundgesetzes.

Wer Literatur zur Vertiefung des Vorlesungsstoffes sucht: Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht (4. Auflage, Oldenbourg-Verlag 2005).

b) Nützliche Websites: www.datenschutz.de; Gesetzestexte findet man auf der Website www.staat-modern.de unter Service.

2. Verfassungsrechtliche Grundlagen

a) Typische **Funktionen der Grundrechte**: (1) **Abwehrrechte** gegen den Staat (Art. 1 Abs.3 GG). Der Bürger ist dabei kein unmittelbarer Adressat. (2) **Schutzpflichten**: Grundrechte geben "Aufträge" an den Staat, bestimmte Schutzstandards zu schaffen. Gesetzgeber muss Grundrechte bei der Schaffung der einfachen Gesetze beachten. Bei der Auslegung der Gesetze sind die Grundrechte ebenfalls zu berücksichtigen. Grundrechte werden also bei grundrechtskonformer Auslegung auch im einfachen Recht wirksam.

Zwischen Bürgern gelten Grundrechte nur "mittelbar", nämlich vermittelt durch das einfache Recht (sogenannte "**mittelbare Drittwirkung**" von Grundrechten).

b) **Schutzwirkung von Grundrechten**: Der **Schutzbereich des Grundrechts** sieht zunächst eine Freiheitsphäre vor, die das Grundrecht schützt. Z.B. garantiert das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu verfügen. Der Staat kann diese grundrechtlich garantierte Freiheit durchaus beschränken. Er muss für einen solchen **Grundrechtseingriff** aber eine **Rechtfertigung** haben. In der Regel beschreibt das Grundgesetz selbst, unter welchen Bedingungen ein Grundrecht eingeschränkt werden darf (sog. Schrankenvorbehalt). Stets jedoch ist Mindestbedingung für eine verfassungskonforme Grundrechtseinschränkung, dass sie durch **Gesetz** erlaubt wird. Dieses Gesetz muss seinerseits im Einklang mit der Verfassung stehen, insbesondere **verhältnismäßig** sein. Greift eine staatliche Behörde oder ein Gericht aufgrund einer gesetzlichen Rechtsgrundlage in ein Grundrecht ein, muss ihr/sein Handeln im Einklang mit dem ermächtigenden Gesetz (und im Einklang mit der Verfassung!) stehen.

c) Grundrechte, die vor **staatlicher Informationsverarbeitung** schützen, sind vor allem das Recht auf informationelle Selbstbestimmung (Art. 2 Abs.1, 1 Abs.1 GG); das Brief- und Fernmeldegeheimnis (Art. 10 Abs.1 GG) und die Unverletzlichkeit der Wohnung (Art. 13 Abs.1 GG). Das **Recht auf informationelle Selbstbestimmung** ist Ausfluss des allgemeinen Persönlichkeitsrechts; es schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe seiner Daten zu verfügen. Das **Brief- und Fernmeldegeheimnis** schützt die Vertraulichkeit von bestimmten Kommunikationsvorgängen. Das Grundrecht auf **Unverletzlichkeit der Wohnung** garantiert die

Wahrung einer räumlichen Privatsphäre. Man kann somit sagen, dass die Grundrechte aus Art. 10 und Art. 13 GG besondere Ausprägungen des allgemeinen Persönlichkeitsrechts darstellen. Der Grundgesetzgeber stellt mit ihnen besonders schutzbedürftige Ausformungen des Persönlichkeitsrechts typisierend unter einen besonderen Schutz.

d) Neben diesen eng miteinander verwandten Grundrechten gibt es grundrechtliche Gewährleistungen, die **in** bestimmten **Einzelfällen** ebenfalls durch staatliche Informationsverarbeitung beeinträchtigt sein können. Beispielsweise ist ein deutscher Staatsbürger in seiner **Versammlungsfreiheit** aus Art. 8 Abs. 1 GG beeinträchtigt, wenn die Polizei ihn bei der Teilnahme an einer Demonstration filmt. Die **Pressefreiheit** wird beeinträchtigt, wenn die Redaktion eines Pressemagazins gezwungen wird, ihre Informationsquellen preiszugeben oder wenn sie eine Durchsuchung ihrer Redaktionsräume durch Strafverfolgungsorgane erdulden muss (BVerfGE 20, 162 - Spiegel). Das **Asylrecht** aus Art. 16a GG wird beeinträchtigt, wenn die Ausländerbehörde durch unbedachte Informationsweitergaben einen Asylbewerber in der Gefahr weiterer Verfolgungen aussetzt usw..

e) Die Grundrechte können durch Bundes- oder Landesgesetze eingeschränkt werden, welche die Informationsverarbeitung von staatlichen Stellen und nichtstaatlichen Stellen regeln. Ob ein **Bundes- oder Landesgesetz** zu verabschieden ist, ist Frage der grundgesetzlichen Verteilung der Gesetzgebungskompetenz (Art. 70 ff. des Grundgesetzes). Sie ist Ausfluss des **Bundesstaatsprinzips**.

f) Das **Recht auf informationelle Selbstbestimmung** wird aus dem Allgemeinen Persönlichkeitsrecht abgeleitet (Art. 2 Abs. 1, Art. 1 Abs. 1 GG, grundlegend hierzu ist das sogenannte **Volkszählungsurteil**: BVerfGE 65, 1). Es schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu verfügen. Dabei können die geschützten Daten unterschiedlichster Natur sein, sie reichen von intimen Tagebuchaufzeichnungen bis zum Namen und seine Verwendung in der Öffentlichkeit.

In das Recht auf informationelle Selbstbestimmung wird **eingegriffen**, wenn der Staat die rechtliche Verpflichtung des Einzelnen begründet, bestimmte Daten zu offenbaren (z.B.: gesetzliche Meldepflicht bei Wohnortwechsel), aber auch, wenn Behörden oder Gerichte personenbezogene Daten erheben, verarbeiten oder nutzen (z.B. Polizeiliche Datenverarbeitung zur Strafverfolgung). Die **freiwillige, ausreichend konkrete Einwilligung** schließt einen Grundrechtseingriff grundsätzlich aus (weil der Betroffene dann über die Preisgabe und Verwendung selbst verfügt!).

Eine Beschränkung des Rechts auf informationelle Selbstbestimmung ist nur **gerechtfertigt**, wenn ein **Gesetz** vorliegt, das genau und verständlich die Anforderungen an den Eingriff beschreibt (Grundsatz der "**Normenbestimmtheit und Normenklarheit**"). Die Rechtsgrundlage ist auch nur verfassungskonform, wenn sie verhältnismäßig ist. **Verhältnismäßigkeit** von Gesetzen heißt im Zusammenhang mit der Ermächtigung zur Datenverarbeitung: die Ermächtigung zur Informationsverwendung muss legitimen Zwecken dienen, hierfür geeignet und erforderlich sein, und auch nicht unangemessen in die Freiheit des Betroffenen eingreifen. Ein besonders schwerwiegender Eingriff liegt z.B. vor, wenn sensible Daten ohne Kenntnis des Betroffenen verwendet werden sollen. Auch muss der Gesetzgeber **organisatorische und verfahrensrechtliche Vorkehrungen** treffen, welche der Gefahr einer Verletzung des Rechts auf informationelle Selbstbestimmung entgegenwirken (dies ist Ausfluss der Schutzpflicht! Siehe oben 2 a). Hierzu gehört z.B. die Einrichtung von unabhängigen **Datenschutzbehörden**, um den Schutz des Bürgers vor ungerechtfertigter Informationsverarbeitung zu gewährleisten.

Werden den ausführenden Stellen (Behörden / Gerichte usw.) **Ermessensspielräume** (so genannte "Kanngesetze") eingeräumt, dürfen sie personenbezogene Daten auch nur unter Beachtung des Grundsatzes der Verhältnismäßigkeit verwenden. Verhältnismäßigkeit heißt dann: Selbst wenn die Voraussetzungen des ermächtigenden Gesetzes zu einer Datenverarbeitung gegeben sind, darf die Stelle Daten nur verarbeiten, wenn dies zur Erfüllung des Gesetzeszweckes geeignet und erforderlich ist und vor allem nicht unangemessen in die Rechte des Betroffenen eingreift.

Fälle zu Abschnitt 2)

Fall 1)

Eine Person B leidet immer wieder unter vorübergehenden Bewusstseinsstörungen. Er ist allerdings nicht geschäftsunfähig, sondern in seiner Geschäftsfähigkeit lediglich eingeschränkt. Für sie ist deshalb eine Betreuung angeordnet (das heißt: Das Amtsgericht bestellt für B einen Betreuer, der B gerichtlich und außergerichtlich vertritt. B als Betreuer bleibt aber handlungs- und geschäftsfähig). B schließt mit einem Wohnungseigentümer W einen Mietvertrag ab und verschweigt dabei den Umstand, dass für ihn eine Betreuung angeordnet ist. Als W hiervon erfährt, ficht er seine Zustimmung zum Mietvertrag wegen arglistiger Täuschung an (dazu: Wortlaut § 123 Abs.1 BGB: "Wer zur Abgabe einer Willenserklärung durch arglistige Täuschung oder widerrechtlich durch Drohung bestimmt worden ist, kann die Erklärung anfechten.").

Fallfrage a) Woraus leitet man das Recht auf informationelle Selbstbestimmung ab und was schützt dieses Grundrecht?

Fallfrage b) Kann sich B gegenüber W auf sein Grundrecht auf informationelle Selbstbestimmung berufen?

Fallfrage c) Wenn nicht, kommt das Grundrecht auf informationelle Selbstbestimmung irgendwie zum Tragen? Durfte W danach seine Erklärung zum Abschluss des Mietvertrags anfechten?

Fall 2)

Nehmen Sie an, die Polizei verarbeitet heimlich personenbezogene Daten eines Betroffenen. Beschreiben Sie die Voraussetzungen, die erfüllt sein müssen, damit dieser Eingriff in das Grundrecht auf informationelle Selbstbestimmung gerechtfertigt ist!

3. Anwendungsbereich des BDSG, Grundbegriffe, Grundprinzipien

a) Ein in der Praxis wichtiges, wenn nicht das wichtigste Gesetz zur Regelung von Datenverarbeitungsbefugnissen ist das **Bundesdatenschutzgesetz (BDSG)**. Vereinfacht ausgedrückt regelt das BDSG den Umgang öffentlicher Stellen des Bundes mit personenbezogenen Daten, bestimmte Fälle des Umgangs öffentlicher Stellen der Länder mit personenbezogenen Daten und die Informationsverwendung durch nichtöffentliche Stellen.

b) Der **Anwendungsbereich des BDSG** ist im Wesentlichen in § 1 Abs.2 BDSG geregelt. Der Umgang mit personenbezogenen Informationen durch **nichtöffentliche Stellen** regelt dabei **§ 1 Abs.2 Nr. 3 BDSG**. Stichwortartig zusammengefasst stellt er folgende Voraussetzungen für die Anwendung des BDSG:

- Adressat: Handelt eine nicht-öffentliche Stelle? Vgl. § 2 Abs.4 BDSG

- Bei Vereinigungen mit privatrechtlicher Rechtsform, z.B. AG, GmbH: § 2 Abs.4 Satz 1 BDSG.
 - Ausnahme: Wahrnehmung hoheitlicher Aufgaben (Beleihung), § 2 Abs.4 Satz 2 BDSG.
 - Ist die öffentliche Hand Träger einer juristischen Gesellschaft des privaten Rechts? Dann sind § 2 Abs.1-3 BDSG zu prüfen (Beispiel: Stadtwerke GmbH).
 - Wird der Staat in Gestalt einer juristischen Person des Öffentlichen Rechts tätig, ist diese juristische Person immer "öffentliche Stelle" im Sinne des § 2 BDSG. Wird diese Stelle wie ein Privatunternehmen auf dem Markt als Wettbewerbsunternehmen tätig, finden trotzdem auch die Regeln über die Datenverarbeitung von nichtöffentlichen Stellen Anwendung (vgl. § 27 Abs.1 Nr. 2b BDSG; Beispiel: Sparkassen - sie verhalten sich auf dem Markt wie "normale Banken").
- Welche Form des Datenumgangs wird erfasst?
- Unter Einsatz von Datenverarbeitungsanlagen
 - in oder aus nicht-automatisierten Dateien

c) Die **wichtigsten Begriffe** des Datenschutzrechts werden in § 2 und § 3 BDSG definiert (bitte lesen!!).

d) Die wichtigsten **datenschutzrechtlichen Prinzipien** dienen teilweise zur Umsetzung der verbindlichen Vorgaben der **Europäischen Datenschutzrichtlinie** (abrufbar unter www.datenschutz-berlin.de unter Europa), sind aber auch verfassungsrechtlich begründet. Hierzu gehört, dass eine Datenverwendung stets durch eine "**bereichsspezifische**" (= hinreichend bestimmte und klare) gesetzliche **Rechtsgrundlage** oder durch eine wirksame Einwilligung erlaubt sein muss. Beispiel: Die polizeilichen Generalklauseln der Länder, die die Polizei allgemein zur Gefahrenabwehr ermächtigen, genügen nicht (mehr) der Anforderung einer bereichsspezifischen gesetzlichen Rechtsgrundlage. Die Verwendung der personenbezogenen Daten ist auf den gesetzlich bestimmten Zweck gebunden (Grundsatz der **Zweckbindung**). Dieses Prinzip kann allerdings durchbrochen werden, wenn der Gesetzgeber solche Zweckänderungen ausdrücklich zulässt. Beispiel: § 28 Abs.1 Nr.1 BDSG erlaubt nichtöffentlichen Stellen die Datenverarbeitung zur Abwicklung eines Vertragsverhältnisses mit dem Betroffenen. Die verantwortliche Stelle darf Adressdaten aber auch zu Werbezwecken nutzen, wenn die Voraussetzungen des § 28 Abs.3 Nr. 3 BDSG erfüllt sind. Eine **Vorratsdatenspeicherung** zu unbestimmten Zwecken ist jedoch wegen des Verstoßes gegen das Zweckbindungsprinzip generell unzulässig.

Fall 3)

Eine Wäscherei W verwendet folgendes Rabattsystem: Der Kunde zahlt für das Waschen von zwanzig Hemden einen (vergünstigten) Betrag im Voraus. Die Wäscherei legt dann eine Kundenkarte an. Diese besteht aus gedruckten Karteikarten, die aus einem Adressfeld und zwanzig Leerfeldern besteht. In das Adressfeld werden handschriftlich der Name und - für etwaig notwendige Rückfragen - die Telefonnummer des jeweiligen Kunden eingefügt. Für jedes gewaschene Hemd wird eines der Leerfelder angekreuzt. Ist die Karte voll, wird sie in Anwesenheit des Kunden zerrissen und auf Wunsch durch eine neue Karte ersetzt. Der jeweilige Name und die Telefonnummer werden von der Wäscherei beim Kunden erfragt und nicht weiter überprüft.

Ist der Anwendungsbereich des BDSG eröffnet?

4. Zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten

a) **Allgemeine Grundregel des Datenschutzrechts:** Eine Datenerhebung, Datenverarbeitung oder Datennutzung ist nur zulässig, wenn sie durch die wirksame Einwilligung des Betroffenen oder durch eine Rechtsvorschrift erlaubt wird (vgl. § 4 Abs.1 BDSG -wichtige Vorschrift! Bitte lesen!!).

Grundsätzlich sind personenbezogene Daten **vorrangig beim Betroffenen** zu erheben (**Grundsatz der Direkterhebung**). Die Datenerhebung ohne Mitwirkung des Betroffenen ist nur unter den Voraussetzungen des § 4 Abs.2 BDSG zulässig. Der Gesetzgeber bringt hierdurch zum Ausdruck, dass nur so schonend wie möglich in die Befugnis des Betroffenen eingegriffen werden darf, über seine Daten grundsätzlich selbst zu verfügen (wenn schon Daten verwendet werden, dann wenigstens unter Mitwirkung des Betroffenen).

Wenn die verantwortliche Stelle Daten beim Betroffenen erhebt, muss sie ihn über bestimmte Umstände der weiteren Datenverwendung, wie z.B. Identität der verantwortlichen Stelle, Zweckbestimmung der Datenverwendung usw. informieren (lesen Sie hierzu § 4 Abs.3 BDSG!). Meines Erachtens ist die **ordnungsgemäße Information des Betroffenen** zumindest regelmäßig Voraussetzung für die Rechtmäßigkeit der weiteren Verwendung der Daten. Abzuleiten ist dies aus einer Erwägung in der EU-Datenschutzrichtlinie, wonach eine ordnungsgemäße Information notwendig ist, um eine Datenverwendung nach Treu und Glauben zu gewährleisten. Diese Frage ist allerdings in der Fachliteratur umstritten.

b) Die **Voraussetzungen** für eine **wirksame Einwilligung** ergeben sich aus § 4a BDSG (lesen!):

(1) Mit dem Begriff der Einwilligung macht der Gesetzgeber kenntlich, dass die Erklärung **zeitlich vor** der beabsichtigten Datenverwendung zu erteilen ist (die Begriffsbestimmung der Einwilligung ergibt sich aus § 183 BGB).

(2) Die Einwilligung in eine Verwendung personenbezogener Daten muss vom Betroffenen freiwillig gegeben werden. Die **Freiwilligkeit** ist nicht nur fraglich, wenn ein Betroffener nur **unter Druck** seine Einwilligung erteilt (Beispiel: Ein Arbeitnehmer willigt in weitgehende Verwendung seiner Daten durch den Arbeitgeber ein, weil er ansonsten befürchtet, entlassen bzw. nicht eingestellt zu werden). Auch dann, wenn die **Einsichts- und Urteilsfähigkeit** des Betroffenen nur eingeschränkt vorliegt, ist die Wirksamkeit der Einwilligung fraglich (Minderjährige / Geistesschwache). Zu prüfen ist dann, ob der Einwilligende die **Tragweite seiner Entscheidung überblicken** kann.

(3) Die Wirksamkeit der Einwilligung hängt auch von einer **vorherigen hinreichenden Information** des Betroffenen über die näheren Umstände der beabsichtigten Datenverwendung ab (lesen Sie dazu § 4a BDSG). Insbesondere wenn besondere Arten personenbezogener Daten verwendet werden sollen, muss der Betroffene ausdrücklich hierin einwilligen (§ 4a Abs.3 BDSG, zum Begriff der besonderen Arten vgl. § 3 Abs.9 BDSG). Die Einwilligung muss so konkret und verständlich gefasst sein, dass der Betroffene die Folgen seiner Einwilligung einschätzen kann. Bei komplexen Verarbeitungsvorgängen genügt es daher oft nicht, dass der Betroffene eine von der verantwortlichen Stelle vorbereitete, lediglich pauschal auf die in § 4a BDSG aufgelisteten Kriterien hinweisende Erklärung unterschreibt.

(4) Grundsätzlich hat die Einwilligung **schriftlich** zu erfolgen (§ 4a Abs.1 Satz 3 BDSG). Das bedeutet, dass der Betroffene eine Unterschrift unter eine verkörperte Erklärung setzt. **Ausnahmen** sind nur zulässig, wenn sie aufgrund **besonderer Umstände** gerechtfertigt sind. Unter den Bedingungen des § 126a BGB kann die Einwilligungserklärung auch **elektronisch** erfolgen.

Aufgepasst! Für den Bereich der Internetnutzung gibt es vorrangige speziellere Vorschriften im Teledienststedatenschutzgesetz (TDDSG) und im Telekommunikationsgesetz (TKG). Dann muss die Einwilligung auf einer eindeutigen und bewussten Handlung des Beteiligten bzw. Nutzers beruhen (opt-in-Lösung) und sie muss protokolliert werden. Außerdem muss der Beteiligte bzw. Nutzer den Inhalt seiner Einwilligung abrufen können.

Das Schriftlichkeitsgebot dient einerseits dazu, die Einwilligungserklärung zu dokumentieren (Beweisfunktion), andererseits dazu, den Betroffenen die Folgen seiner Einwilligung vor Augen zu halten (Warnfunktion). Deshalb darf die verantwortliche Stelle eine vorbereitete Einwilligungserklärung nicht unter anderen rechtsgeschäftlichen Erklärungen "verstecken". Soll die Einwilligung mit anderen Erklärungen verbunden werden, sieht § 4a Abs.1 Satz 4 BDSG ausdrücklich vor, dass sie **hervorzuheben** ist. Dies kann beispielsweise durch Unterstreichung, **Fett**ierung oder durch eine gesonderte Überschrift geschehen (vgl. ausgeteilte Lastschriftinzugsermächtigung).

(5) Grundsätzlich sind Einwilligungen nach § 4a BDSG **frei widerruflich**, allerdings nur mit Wirkung für die Zukunft.

(6) Bei standardisierten Erklärungen wird das BDSG durch Schutzvorschriften des **Rechts der Allgemeinen Geschäftsbedingungen** ergänzt (lesen Sie §§ 305-310 BGB).

c) Ohne eine Einwilligung des Betroffenen ist die Verwendung personenbezogener Daten nur zulässig, wenn sie durch eine **Rechtsvorschrift** erlaubt wird.

Der Begriff der Rechtsvorschrift ist in einem **materiellen Sinne** zu verstehen. Dem entsprechend sind nicht nur durch das Parlament verabschiedete Gesetze, sondern z.B. auch Rechtsverordnungen Rechtsvorschriften im Sinne des § 4 Abs.1 BDSG. Für **Tarifverträge** gilt entsprechendes, weil § 4 des Tarifvertragsgesetzes dem Tarifvertrag gesetzesähnliche Wirkungen zuschreibt. Die Rechtsprechung hat anerkannt, dass **Betriebsvereinbarungen** als Rechtsvorschriften gelten. Allerdings müssen sie mit höherem Recht im Einklang stehen. Das bedeutet: Sie müssen einen datenschutzrechtlichen Mindestschutzstandard gewährleisten, der mit dem gesetzlichen Schutzstandard in etwa vergleichbar ist. **Keine Rechtsvorschriften** sind **Verträge** zwischen der verantwortlichen Stelle und dem Betroffenen. Zwar legen die Vertragsparteien in einem Vertrag bestimmte Rechte und Pflichten fest, diese binden jedoch regelmäßig nicht dritte Personen, was ein typisches Merkmal von Rechtsvorschriften ist.

Bei der Anwendung von Rechtsvorschriften ist der Grundsatz der Direkterhebung zu beachten (siehe oben unter a)). Beispiel für eine Direkterhebung im Arbeitsverhältnis: Personalfragebogen bei Bewerbungen. Beispiel für die Datenerhebung ohne Mitwirkung des betroffenen Mitarbeiters: Überwachung eines Mitarbeiters durch eine Detektei.

Exkurs: Fragerecht des Arbeitgebers bei Bewerbungen (häufig nicht vom BDSG erfasst)!
In der Situation der Bewerbung ist zu beachten, dass der Arbeitgeber in seinem **Fragerecht** auf solche Fragen eingeschränkt ist, für die er ein **berechtigtes, billigenwertes und schützenswertes**

Interesse im Hinblick auf die Tätigkeit und den Arbeitsplatz hat. Überschreitet der Arbeitgeber den zulässigen Rahmen, ist die Frage rechtswidrig. Der Stellenbewerber hat dann das **Recht zur Lüge**. Stellt der Arbeitgeber später fest, dass die Antworten des Bewerbers auf unzulässige Frage unrichtig waren, steht ihm - anders als bei zulässigen Fragen - kein Recht zu, den Arbeitsvertrag wegen arglistiger Täuschung nach § 123 BGB anzufechten. Typische Beispiele für unzulässige, bzw. problematische Fragen: Fragen nach speziellen Familienverhältnissen (Heiratsabsicht, sexuelle Neigungen usw.), Vorstrafen (zulässig bei sicherheitsrelevanten Berufen, z.B. Kassierer), Gesundheitsdaten, genetische Dispositionen, Schwangerschaft, Gewerkschaftszugehörigkeit oder Religionszugehörigkeit (zulässig bei so genannten Tendenzbetrieben).

d) Gibt es **gesetzliche Datenverarbeitungsvorschriften außerhalb des BDSG**, die eine Verwendung personenbezogener Daten spezieller als das BDSG regeln, finden sie vorrangig Anwendung (vgl. § 1 Abs.3 BDSG). Das bedeutet für Sie: Bevor Sie prüfen, ob eine Datenverwendung nach dem BDSG zulässig ist, müssen Sie zunächst einmal prüfen, ob es nicht Spezialgesetze gibt, die eine Datenverwendung anders wie das BDSG regelt. Typische Beispiele: Die Datenverwendung im Zusammenhang mit Telekommunikationsvorgängen wird speziell vom TKG geregelt. Im Bezug auf die Nutzung des Internet können TDDSG und TKG gegenüber dem BDSG speziellere Regelung enthalten. In Bezug auf Verträge gibt es teilweise Spezialvorschriften im BGB (z.B. Überweisungsauftrag). Die § 915 ff. ZPO und die Schuldnerverzeichnis-Verordnung (SchuVVO) regeln die Verwendung von Daten aus sogenannten Schuldnerverzeichnissen, die bei den Amtsgerichten geführt werden usw..

e) Fehlt eine solche spezielle vorrangige Regelung, muss man prüfen, ob eine Rechtsvorschrift im BDSG die Datenverwendung erlaubt.

Im Ersten Abschnitt des BDSG ("Allgemeiner Teil") finden Sie Rechtsvorschriften, die spezielle Formen der Verarbeitung für öffentliche und nichtöffentliche Stellen gleichermaßen regeln. Nicht alle Regeln ermächtigen zu einer Datenverarbeitung, sondern ergänzen nur die Verarbeitungsregeln im Zweiten bzw. Dritten Abschnitt. Hier ein kurzer, stichwortartiger Überblick:

- **automatischen Einzelentscheidung** (§ 6a BDSG)
- **Videoüberwachung** (§ 6b BDSG)
- **mobile personenbezogene Speicher- und Verarbeitungsmedien** (Chipkarten, § 6c BDSG)
- **Gemeinsamer Abruf** (§ 10 BDSG)
- **Datentransfer in so genannten Drittstaaten** §§ 4b, c

f) Meistens allerdings werden Sie bei der Prüfung der Rechtmäßigkeit einer Datenverwendung durch nichtöffentliche Stellen auf die Datenverarbeitungsregeln im Dritten Abschnitt des BDSG (§§ 27 ff. BDSG) zurückgreifen müssen.

§ 27 BDSG ermächtigt nicht zur Datenverarbeitung, sondern beschreibt, für welche Fälle der Datenverwendung der Dritte Abschnitt Anwendung findet.

Die **wichtigsten Datenverarbeitungsregeln sind in § 28 und § 29 BDSG** vorgesehen. Dabei regelt § 28 BDSG die Verwendung von personenbezogenen Daten zu eigenen Geschäftszwecken, § 29 BDSG hingegen die geschäftsmäßige Erhebung und Speicherung zum Zweck der Datenübermittlung. **Voneinander abzugrenzen** sind § 28 und § 29 nach dem jeweiligen **Verarbeitungszweck**: Erhebt eine Stelle Daten, um sie (auch) für sich zu verwenden, ist § 28 BDSG anzuwenden; § 29 BDSG kommt dann als Erlaubnisvorschrift für die fragliche Datenverwendung nicht

in Betracht. Erhebt und verarbeitet eine Stelle personenbezogene Daten ausschließlich mit dem Ziel, sie anderen Stellen (z.B: Kunden) zur Verfügung zu stellen, dann kommt § 29 BDSG als Erlaubnisvorschrift in Betracht. Beispiele:

- Eröffnet ein Kunde bei einer Sparkasse ein Girokonto und verarbeitet die Sparkasse zur Vertragserfüllung personenbezogene Daten, ist § 28 BDSG anzuwenden (die Datenverarbeitung geschieht nicht, um die Daten an Dritte zu übermitteln, selbst wenn eine Datenübermittlung hin und wieder anlassbezogen erfolgt).
- Sammelt und speichert eine Wirtschaftsauskunftei oder die Schufa personenbezogene Daten von Verbrauchern, um diese Daten an Kunden zu übermitteln, ist § 29 BDSG zu prüfen (die Daten werden ausschließlich für die Datenübermittlung erhoben und aufbereitet. Die Auskunftei / Schufa hat keinerlei inhaltliches Interesse an den Daten).
- Ein Unternehmen beauftragt eine Detektei um herauszufinden, ob ein krank geschriebener Arbeitnehmer tatsächlich erkrankt ist oder nur "simuliert". Die Detektei beobachtet den betroffenen Arbeitnehmer und gibt die Beobachtung per eMail an den Arbeitgeber weiter: Die Datenbeschaffung durch den Arbeitgeber ist nach § 28 BDSG zu beurteilen (der Arbeitgeber will die Daten für eigene Geschäftszwecke, nämlich zur Klärung von Personalangelegenheiten). Die Datenverarbeitung der Detektei hingegen richtet sich nach § 29 BDSG (die Detektei sammelt und verwendet die Daten nur, um sie ihrem Auftraggeber zur Verfügung zu stellen!).

g) Zu § 28 Abs.1 Nr. 1 BDSG erlaubt die Datenverwendung zur Erfüllung eines Vertrags oder vertragsähnliches Vertrauensverhältnisses mit dem Betroffenen (Achtung! Unabdingbare Rechte (§ 6 BDSG) dürfen vertraglich nicht ausgeschlossen werden!). Hier stichwortartig die Prüffolge:

(1) Vertrag

Gemeint ist Vertrag mit dem Betroffenen, nicht mit Dritten. Probleme z.B. bei modernen Joint Ventures

(2) Liegt ein vertragsähnliches Vertrauensverhältnis vor?

- o ja bei Vertragsanbahnung
- o ja bei Datenverwendung zur Erfüllung eines Vereinszweckes, wenn Betroffener ein Vereinsmitglied ist
- o nein bei Vorbereitung der Ansprache zu Werbezwecken, weil aufgedrängte Datenverarbeitung. Außerdem spricht die Existenz des § 28 Abs.3 Nr. 3 BDSG gegen ein Vertrauensverhältnis.

(3) Die Datenverwendung nach § 28 Abs.1 Nr.1 BDSG ist nur zulässig, wenn sie **erforderlich** für den jeweiligen Zweck des Vertrags bzw. vertragsähnlichen Vertrauensverhältnisses ist.

h) Zu § 28 Abs.1 Nr. 2 BDSG: Diese Vorschrift verlangt eine **Interessenabwägung zwischen dem Interesse der verantwortliche Stelle an der Verwendung der Daten und dem schutzwürdigen Interesse des Betroffenen**, dass die Daten nicht (oder nicht so) verwendet werden.

Stichwortartige Prüffolge:

- Liegt ein **berechtigtes Interesse** der verantwortlichen Stelle vor? Berechtigtes Interesse wird üblicherweise weit verstanden: "jedes nach vernünftiger Erwägung durch die Sachlage gerechtfertigtes Interesse". Das Interesse muss von der Rechtsordnung gebilligt sein. Beispiele:

- o Ja bei wirtschaftlichem Interesse;
- o Nein bei bloßer Neugier,
- o Nein bei Missbrauchsabsicht (Schädigung des Betroffenen durch üble Nachrede usw.).

- Ist die Verwendung der personenbezogenen Daten **erforderlich**, um die berechtigten Interessen zu verfolgen? Gegeben, wenn die berechtigten Interessen nicht ohne die Kenntnis der Daten (vernünftig) gewahrt werden können.

- Stehen der Verwendung **schutzwürdige Interessen des Betroffenen entgegen**? Schutzwürdige Interessen zielen zum einen auf den Schutz der Privat-, Intim- oder Vertraulichkeitssphäre des Betroffenen ab, können aber auch andere Gesichtspunkte betreffen (z.B. zu befürchtende wirtschaftliche oder berufliche Nachteile).

Ob die berechtigten Interessen der verantwortlichen Stelle oder die schutzwürdigen Interessen des Betroffenen vorrangig sind, kann nur im Wege der **Interessenabwägung** ermittelt werden.

Beispiele für mögliche Kriterien:

- o Welche **Art und welcher Inhalt** von Daten werden verwendet? Reichen sie in den Intimbereich oder sehr weit in die Privatsphäre hinein? => große Schutzbedürftigkeit des Betroffenen. Sind sie ihrer Natur nach risikoträchtig => eher große Schutzbedürftigkeit. Wenig risikoträchtige Daten => eher eine geringe Schutzbedürftigkeit, es ist aber auf den Zusammenhang der Datenverwendung zu achten! (Beispiel: die Adresse eines Betroffenen ist in der Regel ein "harmloses" Datum, wie auch § 28 Abs.1 Nr. 3 BDSG zeigt. Gerade aber wenn ein Betroffener dafür Sorge trägt, dass die Adresse nicht allgemein bekannt gegeben wird, können besondere schutzwürdige Interessen vorliegen, wie etwa eine besondere Gefährdung des Betroffenen).
- o Im welchen **Umfang** sollen Daten verwendet werden? Faustformel: Je mehr Daten über eine Person verwendet werden sollen, umso mehr spricht dies für ein starkes schutzwürdiges Interesse gegen die Datenverwendung (Beispiel: DataWarehouse und DataMining-Systeme).
- o Welches **Gewicht** kommt dem **Verwendungsinteresse** zu? Hat die verantwortliche Stelle nur ein relativ wenig schutzwürdiges wirtschaftliches Interesse (etwa Datenverwendung zu Werbezwecken) oder dient die Datenverwendung zu Selbstschutzzwecken? usw.

i) 28 Abs.1 Nr. 3 BDSG regelt die Verwendung von **allgemein zugänglichen Daten**; gemeint sind damit z.B. Daten aus dem Telefonbuch, aber auch aus dem Internet. In einem solchen Fall ist die Datenverwendung unter leichteren Bedingungen zulässig. Ausnahme: Es steht ein offensichtlich schutzwürdiges Interesse des Betroffenen der Datenverwendung entgegen.

k) Ein zentrales datenschutzrechtliches Prinzip ist das sogenannte **Zweckbindungsprinzip**. Deshalb sieht § 28 Abs.1 Satz 2 BDSG vor, dass bei der Datenerhebung die Verwendungszwecke konkret festzulegen sind. Im BDSG ist dieser Grundsatz jedoch stark durchbrochen. Personenbezogene Daten dürfen unter den Bedingungen des § 28 Abs.2, Abs.3 BDSG auch zu anderen als den ursprünglichen Zwecken verwendet werden.

l) Dazu gehört auch die **Datennutzung und Datenweitergabe an Dritte**, die in § 28 Abs.3 BDSG geregelt ist. Die Datenempfänger sind grundsätzlich an den Zweck gebunden, zu dem ihnen die Daten übermittelt worden sind (lesen Sie dazu § 28 Abs.5 BDSG).

Die Datennutzung und Datenübermittlung gemäß § 28 Abs.3 BDSG ist zulässig:

- nach Nr.1: wenn sie zur Wahrung **berechtigter Interessen Dritter** erforderlich ist, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein **schutzwürdiges Interesse** an dem Ausschluss an der Übermittlung hat (die Prüfung erfolgt ganz ähnlich wie bei § 28 Abs.1 Nr. 2 BDSG);

- nach Nr.2: wenn sie zur **Gefahrenabwehr oder zur Strafverfolgung** erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss an der Übermittlung hat;

- nach Nr.3: zu Zwecken der **Werbung und Markt- und Meinungsforschung**, wenn nur die Daten verwendet werden, die in Abs.3 Nr.3 aufgelistet sind **und kein** Grund zu der Annahme besteht, dass der Betroffene ein **schutzwürdiges Interesse** an dem Ausschluss an der Übermittlung hat.

Achtung! § 28 Abs.4 BDSG ist zu beachten: Der Betroffene hat ein Recht, der Ansprache zu Wer-

bezwecken oder zu Zwecken der Markt- und Meinungsforschung zu widersprechen, dann hat die Nutzung oder Übermittlung zu unterbleiben. Bei der Ansprache muss die verantwortliche Stelle den Betroffenen auf das **Widerspruchsrecht** hinweisen und ihm den Widerspruch durch die Angabe der hierfür notwendigen Kontaktadresse ermöglichen. Nach § 28 Abs.3 Satz 2 BDSG liegt stets ein überwiegendes schutzwürdiges Interesse vor, wenn die Daten aus einem Vertragsverhältnis oder vertragsähnlichem Vertrauensverhältnis stammen, die sich auf strafbare oder ordnungswidrige Verhaltensweisen beziehen. Das gleiche gilt, wenn der Arbeitgeber Daten über seine Arbeitnehmer übermitteln will.

Exkurs:

"Dritte" im Sinne des § 28 Abs.3 BDSG sind nicht **Auftragsdatenverarbeiter**. Sie werden ganz ähnlich wie Arbeitnehmer der verantwortlichen Stelle behandelt. Lesen Sie dazu § 11 BDSG: Für ein Auftragsdatenverarbeitungsverhältnis müssen zahlreiche Bedingungen erfüllt sein. Der Auftragsdatenverarbeiter hat **in der Regel keine eigenen Verantwortungsspielräume** bei der Durchführung der beauftragten Datenverarbeitung; jeder vorzunehmende Verarbeitungsschritt wird von dem Auftraggeber (schriftlich) vorgegeben. Typisches Beispiel: Aktenvernichter.

m) Achten Sie bitte darauf, dass die **Datenverwendung bei besonderen Arten personenbezogener Daten nur sehr eingeschränkt zulässig ist !** Die Vorschriften des § 28 Abs.1-3 BDSG werden hierdurch erheblich eingeschränkt. **Lesen Sie dazu § 28 Abs.6-9 BDSG (prüfungsrelevant!).**

n) **§ 29 Abs.1 BDSG** setzt **das geschäftsmäßige Erheben, Speichern oder Verändern zum Zwecke der Datenübermittlung** voraus. Die Vorschrift nennt typische Formen der Tätigkeit, die unter § 29 fallen können: Werbung, Auskunftstätigkeit, Adresshandel, Markt- und Meinungsforschung. Achten Sie bitte auf Parallelen und auf Unterschiede zu § 28 Abs.1 BDSG:

- Ähnlich wie bei § 28 Abs.1 Nr.2 ist eine Datenerhebung und Datenspeicherung nur nach Abwägung zwischen Interessen der verantwortlichen Stelle und dem schutzwürdigen Interesse des Betroffenen erforderlich.
- Unterschied: Der Gesetzgeber geht davon aus, dass die geschäftsmäßige Datenbeschaffung und -speicherung zum Zweck der Datenübermittlung ein grundsätzlich berechtigtes Interesse darstellt; das berechtigte Interesse und die Erforderlichkeit der Datenverwendung sind nicht gesondert zu überprüfen! Diese Vorschrift stellt einen großen Erfolg der Direktmarketing- und Auskunftelobby im Gesetzgebungsverfahren dar, ist aber datenschutzrechtlich problematisch, weil bestimmte wirtschaftliche Interessen pauschal als berechtigt anzuerkennen sind, ohne dass insoweit der konkrete Sachzusammenhang zu prüfen ist.
- Ähnlich wie bei § 28 Abs.1 Nr. 3 ist die Datenerhebung und Datenspeicherung dann rechtlich einfacher möglich, wenn die Daten allgemein zugänglich sind.
- Auch das kann datenschutzrechtlich problematisch sein, weil die Tätigkeit der Unternehmen nach § 29 BDSG häufig darin besteht, diese allgemein zugänglichen Daten mit nichtzugänglichen Daten zu verknüpfen. Damit gewinnen die allgemein zugänglichen Daten erheblich an Gefährlichkeit für den Betroffenen.
- In § 29 BDSG werden nur die Erhebung, Speicherung, Veränderung und Übermittlung von personenbezogenen Daten erlaubt. Demgegenüber gestattet § 28 BDSG auch die Nutzung.

Wie bei § 28 Abs.1 BDSG sind die beabsichtigten Verarbeitungszwecke bei der Datenerhebung konkret festzulegen.

Vollziehen Sie anhand des nachfolgenden Beispiels § 29 Abs.1 BDSG nach (*kursive Klammerzusätze*):

Ein Adresshandelsunternehmen kauft von einer Handelskette eine Liste mit den personenbezogenen Daten ihrer Kunden (=Datenerhebung) und pflegt sie in ihren Datenbestand ein (=Datenspeicherung). Ermittelt sie, dass ein Betroffener umgezogen ist, arbeitet sie auch die damit verbundene Adressänderung ein (=Datenveränderung). Erfährt nun ein Betroffener von dieser Tätigkeit und widerspricht der Verwendung der Daten, ist regelmäßig von einem überwiegenden schutzwürdigen Interesse des Betroffenen (=> § 29 Abs.1 Nr.1 bzw. 2 BDSG) auszugehen (**Frage**: warum? Lesen Sie bitte dazu § 29 BDSG komplett!).

- o) § 29 Abs.2 BDSG erlaubt die Datenübermittlung an Dritte. Hier sind nach dem Gesetzeswortlaut "relativ strenge" Maßstäbe zu beachten:
 - o in der Regel muss der Datenempfänger **glaubhaft darlegen**, dass er ein **berechtigtes Interesse am Erhalt der Daten** hat. Das ist nachvollziehbar: § 29 Abs.2 Nr. 1 BDSG gilt nur für die Stelle, welche die Daten übermitteln will! Für den Datenempfänger gilt regelmäßig § 28 Abs.1 Nr. 2 BDSG (oder § 28 Abs.1 Nr.1 BDSG, z.B., wenn es um den Abschluss eines konkreten Vertrags geht).
 - o *Beachten* Sie dabei § 29 Abs.2 Satz 3: In der Regel muss der geschäftsmäßige Datenübermittler die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung dokumentieren (anderes gilt nur bei automatisierten Abrufverfahren: dort obliegt die Aufzeichnungspflicht dem Abrufenden, vgl. § 29 Abs.2 Satz 4 BDSG).
 - o Wenn die Daten aus **allgemein zugänglichen Quellen** entnommen werden können, ist die Datenübermittlung wieder unter vereinfachten Bedingungen zulässig. Auch hier gilt wieder die Ausnahme: Offensichtlich entgegenstehende **schutzwürdige Interessen** hindern die Datenübermittlung (wie bei § 28 Abs.1 Nr.3 BDSG).
 - o *Beachten* Sie dabei § 29 Abs.2 Satz 2 BDSG, der auf § 28 Abs.3 Satz 2 BDSG verweist (ein überwiegendes schutzwürdiges Interesse ist anzunehmen, wenn die Daten aus einem Vertragsverhältnis oder vertragsähnlichem Vertrauensverhältnis stammen, die sich auf strafbare oder ordnungswidrige Verhaltensweisen beziehen. Das gleiche gilt, wenn der Arbeitgeber Daten über seine Arbeitnehmer übermitteln will)

Im Übrigen umfasst § 29 BDSG noch folgende weitere Regelungen: § 29 Abs.3 BDSG enthält Sonderregelungen zur Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen- oder vergleichbare Verzeichnisse. Die entsprechende Geltung der § 28 Abs.4-9 BDSG wird angeordnet. Hier wird die unter Abschnitt n) ganz am Ende aufgeworfene **Frage** beantwortet: Widerspricht der Betroffene einer Verwendung der Daten bei einem Adresshändler, der diese Daten zu Werbezwecken weiterverkaufen will, gilt über § 29 Abs.4 BDSG auch § 28 Abs.4 Satz 1 BDSG entsprechend.

Fälle und Verständnisfragen zu Abschnitt 4)

Frage 4)

a) Nennen Sie "Rechtsvorschriften" im Sinne des § 4 I BDSG, die nicht förmliche Gesetze sind! Gibt es für solche Rechtsvorschriften eine Wirksamkeitsbedingung?

b) Nennen Sie ein Beispiel für Regelungen, die keine Rechtsvorschrift im Sinne des § 4 I BDSG darstellen! Warum stellt das von Ihnen gewählte Beispiel keine Rechtsvorschrift dar?

Fall 5)

Soweit die in den nachfolgenden Sätzen 1-10 beschriebenen Handlungen der B und K datenschutzrechtlich relevant sind, benennen Sie bitte die Handlungen der B und K mit den datenschutzrechtlichen Fachbegriffen und ordnen Sie sie konkret einschlägigen Vorschriften in §§ 28, 29 BDSG zu! Falls Sie meinen, dass der jeweilige Satz keine datenschutzrechtlich relevante Handlung der B und K enthält: Kennzeichnen Sie dies (z.B. mit einem X):

Satz 1: Ein Kunde K beantragt bei der Bank B ein Girokonto mit Überziehungsmöglichkeit.

Satz 2: Die Bank holt vor dem Vertragsabschluss eine Schufa-Auskunft ein.

Satz 3: Außerdem bezieht die B so genannte Schuldnerverzeichnislisten, die nach der Zivilprozessordnung nur an Gewerbetreibenden mit berechtigten Verarbeitungsinteressen weitergegeben werden.

Satz 4: Darin sind Informationen über Personen aufgelistet, die eine Insolvenz erlitten haben, die eine eidesstattliche Versicherung über ihre Vermögensverhältnisse abgegeben haben oder gegen die wegen Nichtbezahlung eines titulierten (=durch Zwangsvollstreckung durchsetzbaren) Anspruchs ein Haftbefehl vorliegt.

Satz 5: Die B überprüft anhand dieser Listen, ob der K in dem Schuldnerverzeichnis steht.

Satz 6: Das ist nicht der Fall.

Satz 7: Der Vertrag wird abgeschlossen.

Satz 8: Wenig später schreibt die B den K an und weist ihn auf eigene Produkte hin (z.B. auf ein Sparbuch mit besonders guter Verzinsung).

Satz 9: Der K ruft bei der B an und teilt ihr mit, dass er weitere Informationen nicht wünscht.

Satz 10: Darauf hin trägt der Datenschutzbeauftragte der B bei dem Datensatz des K einen entsprechenden Vermerk ein.

5. Transparenzregeln und Rechte des Betroffenen

Lesen Sie hierzu die §§ 4 Abs.3, 6, 33, 34, 35 BDSG! Diese Vorschriften sind die wichtigsten Regeln zu den Informationspflichten der verantwortlichen Stellen und Rechten der Betroffenen.

Hinsichtlich der Transparenzregeln kennen Sie bereits eine Pflicht der verantwortlichen Stelle, nämlich die Unterrichtung über das Widerspruchsrecht bei der Ansprache zu Werbezwecken. Die **Information des Betroffenen** durch Benachrichtigung (§ 33 BDSG), Unterrichtung (§ 4 Abs.3, § 4a Abs.1 Satz 2 BDSG) oder Auskunfterteilung (§ 34 BDSG) dienen zur Verwirklichung der **grundsätzlichen Verfügungsbefugnis** des Betroffenen.

Zugleich setzen sie den Betroffenen in die Lage, auf eine **Löschung oder Sperrung** seiner Auffassung nach rechtswidrig gespeicherten Daten oder auf die **Berichtigung** unrichtiger Daten hinzuwirken (vgl. § 35 BDSG).

6. Elemente einer datenschutzgerechten Datenschutzorganisation im BDSG

Aus den vorangegangenen Abschnitten geht hervor, dass die Interessen der verantwortlichen Stellen, bestimmte personenbezogene Daten zu verwenden, manchmal gegenüber den schutzwürdigen Interessen zurückstehen müssen. Da zunächst der Datenverarbeiter die Interessenabwägung vorzunehmen hat, ist zu befürchten, dass er sie regelmäßig zu seinen Gunsten ausfallen lässt. Doch

selbst wenn der Verarbeiter gutwillig ist, fallen Abwägungsvorgänge manchmal schwer, weil besondere, schutzwürdige Belange des Betroffenen für den Datenverwender nicht erkennbar sind.

Deshalb sieht das BDSG "**organisatorischen und verfahrensrechtlichen Maßnahmen**" vor, die dazu beitragen sollen, eine datenschutzgerechte Informationsverarbeitung zu sichern. Hierzu gehören Verfahrensregeln wie zum Beispiel die Festlegung von konkreten Verarbeitungszwecken anlässlich der Datenerhebung (§ 28 Abs.1 Satz 2 BDSG), aber auch die Regeln zur betrieblichen Datenschutzorganisation. Hinzu kommen Regeln über eine externe Datenschutzaufsicht. Man kann hierzu auch die Transparenzregeln zählen (vgl. Abschnitt 5).

a) Folgende Elemente einer **betrieblichen Datenschutzorganisation** sind im BDSG ausdrücklich vorgesehen:

- Meldepflicht und Verfahrensübersicht (§§ 4d, 4e BDSG)
- Betrieblicher Datenschutzbeauftragter (§§ 4f, g BDSG)
- Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5 BDSG)
- Die Schulung von Mitarbeitern (§ 4g Abs.1 Nr.2 BDSG)
- Die Vorabkontrolle (=vorsorgliche Rechtmäßigkeitskontrolle bei Neueinrichtung von risikoträchtigen Verarbeitungssystemen, § 4d Abs.5, 6 BDSG.)
- Laufende Kontrolle der Anwendung von Datenverarbeitungsprozessen (§ 4g Abs.1 Nr. 1 BDSG)
- Technische und organisatorische Maßnahmen zur Datensicherheit (§ 9 BDSG, lesen Sie dazu auch den Anhang zu § 9 BDSG am Ende des BDSG!).

Wenn Sie die mitaufgelisteten Vorschriften aufmerksam gelesen haben, werden Sie feststellen, dass viele Aufgaben zur Gewährleistung einer datenschutzkonformen Datenverwendung dem **betrieblichen Datenschutzbeauftragten** übertragen werden. Er berät sowohl die Leitung der verantwortlichen Stelle, als auch die Betroffenen. Die Effektivität der gesetzlich vorgeschriebenen Maßnahmen hängt also stark davon ab, wie kompetent der Datenschutzbeauftragte ist...

Ein wichtiges Element der betrieblichen Datenschutzorganisation ist gesetzlich nicht vorgesehen: das der "Datenschutzphilosophie", "Privacy Policy" oder Zielsetzung. Besteht in einem Unternehmen eine **Grundsensibilität** für datenschutzrechtliche Belange, garantiert dies oft eher die Einhaltung der Verarbeitungsregeln als die buchstabengetreue Umsetzung des Gesetzeswortlauts ohne Berücksichtigung der eigentlichen Zielsetzung. Das leitet über zu dem Thema, wie ein moderner Datenschutz auszusehen hat.

7. Moderner Datenschutz

Moderner Datenschutz berücksichtigt den Umstand, dass die Datenverarbeitung zunehmend von **stetig kleiner werdenden Datenverarbeitungsträgern** erfolgt und die Informationsverarbeitung sich immer weitergehender **vernetzt**. Diese Entwicklung bringt hinsichtlich des Rechts auf informationelle Selbstbestimmung des Betroffenen eine Vielzahl neuer Gefährdungen mit sich. Nachfolgend werden nur einige Aspekte des modernen Datenschutzes aufgeführt.

a) Der **Selbstdatenschutz** ist zu stärken. Seine Grundidee besteht darin, dass nicht nur der Staat die Verantwortung für die Durchsetzung des Datenschutzes trägt, sondern der Bürger und Unter-

nehmen durch technische Hilfsmittel und durch Infrastrukturleistungen in die Lage versetzt sind, ihre informationelle und kommunikative Selbstbestimmung selbst zu schützen.

Wichtiges Beispiel: **Vermeidung des Personenbezugs** bei der Datenverarbeitung. Das BDSG sieht hierzu in § 3a die Grundsätze der **Datenvermeidung und Datensparsamkeit** vor. Vor allem im Internet soll der Nutzer die Möglichkeit haben, sich **anonym oder pseudonym** im Internet zu bewegen. Deshalb sieht § 4 Abs. 6 TDDSG vor, dass Telediensteanbieter im Rahmen der Zumutbarkeit die anonyme und pseudonyme Nutzung der Teledienste ermöglichen sollen (in der Praxis kommt dies selten vor, weil Anbieter zumeist die Zumutbarkeit verneinen. Infos: www.datenschutzzentrum.de unter dem Stichwort AN.ON).

b) Weiteres häufiges Stichwort: Systemdatenschutz. Er umfasst Ansätze, Rechtsregeln zum Schutz des Rechts auf informationelle Selbstbestimmung in Datenverarbeitungssysteme zu integrieren. Das BDSG sieht hierzu nur wenige Ansätze vor, hierzu gehören z.B. die bereits erwähnten Grundsätze der Datenvermeidung und Datensparsamkeit (spätestens jetzt sollten Sie § 3a BDSG lesen!), aber auch die Vorabkontrolle nach § 4d Abs.5 BDSG.

c) Stärkung der Eigenverantwortlichkeit der verantwortlichen Stellen und Akzentsetzung auf **vorbeugende Datenschutzmaßnahmen.** Dazu gehört das Setzen wirtschaftlicher Anreize für die Einrichtung präventiver Datenschutzkontrollen. Zu nennen ist beispielsweise das **Datenschutzaudit/Datenschutzgütesiegel**, das auf Bundesebene noch nicht existiert (§ 9a BDSG benennt ein solches Datenschutzaudit, sieht aber zugleich ein Umsetzungsgesetz vor, das noch nicht ergangen ist). Daher haben einige Landesgesetzgeber Datenschutzauditregelungen erlassen (falls Sie Informationen suchen: www.datenschutzzentrum.de unter "Datenschutzgütesiegel" und "Datenschutzaudit"). Die Stellen unterziehen sich freiwillig einer externen Datenschutzprüfung und erhalten, wenn sie bestimmte Datenschutzstandards erreichen, ein Datenschutzgütesiegel. Hiervon versprechen sie sich verbesserte Wettbewerbsbedingungen (z.B. bevorzugte Berücksichtigung bei öffentlichen Aufträgen; Werbeeffekte).