Unabhängiges Landeszentrum für Datenschutz:

Änderungsbedarf des Bundesdatenschutzgesetzes (BDSG)

Version vom 24.09.2008

Vorbemerkung

Die folgenden Änderungsvorschläge können nur die Defizite und Regelungslücken des derzeitigen Systems des Datenschutzes verringern. Angezeigt wäre eine grundlegende Reform des Datenschutzrechts in Deutschland, da die Konzepte, die heute in den Datenschutzgesetzen beschrieben werden, auf dem System der Datenverarbeitung aus den 90iger Jahren beruhen. In diese Reform sollten auch die Informationsfreiheitsgesetze, Umwelt- und Verbraucherinformationsgesetze integriert sowie ein Arbeitnehmerdatenschutzgesetz geschaffen werden.

1. Verfassungsrechtlicher Änderungsbedarf

Eine wirksame und effiziente Tätigkeit der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich setzt deren rechtliche, funktionale und materielle Unabhängigkeit voraus. Dies könnte verfassungsrechtlich geregelt werden und sollte in eine Grundgesetzregelung münden. Durch diese sollte die **Unabhängigkeit und eine ausreichende Ausstattung (institutionelle Absicherung) der Datenschutzkontrolle** gewährleistet werden. Viele Aufsichtsbehörden in den Bundesländern sind in die Innenverwaltung integriert. Damit wird die Unabhängigkeit der Datenschutzkontrolle mit einem Fragezeichen versehen. Denn die Aufsicht wird damit politischen Einflüssen ausgesetzt, die im Einzelfall einer effektiven Aufsicht entgegenstehen. Eine unabhängige Datenschutzaufsicht ist, so das Bundesverfassungsgericht, „von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung“ (BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419, 423).

Die völlige Unabhängigkeit der Aufsichtsbehörden verlangt letztlich auch Art. 28 Abs. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Gegen die Bundesrepublik Deutschland hat die EU-Kommission wegen der fehlenden Unabhängigkeit der Aufsichtsbehörden ein Vertragsverletzungsverfahren eingeleitet. Nach Auffassung der Kommission hat die Bundesrepublik dadurch gegen ihre Umsetzungspflicht der Richtlinie aus Art. 249 EG-Vertrag verstoßen.

2. Vollzugspraxis

a) Sanktionsmittel

Die bisherigen Sanktionsmittel müssen ergänzt und Regelungslücken geschlossen werden. So können nach herrschender Rechtsauffassung die Aufsichtsbehörden derzeit keine **Untersagungen für unzulässige Verfahren** der Erhebung, Verarbeitung und Nutzung personenbezogener Daten aussprechen. § 38 Abs. 5 BDSG regelt lediglich die Untersagung von Verfahren, wenn technische und organisatorische Mängel festgestellt wurden. Die Beschränkung des § 38 Abs 5 BDSG, nur Anordnungen durch Verwaltungsakt zu Datensicherheit (§ 9 BDSH und Anlage) treffen zu können, sollte aufgehoben werden. Die Aufsichtsbehörden müssen ermächtigt werden, auch materiellrechtlich datenschutzrechtswidrige Verfahren untersagen zu können. Die gilt vor allem dann, wenn das geplante oder bereits betriebene Verfahren mit einer besonderen Gefährdung des Persönlichkeitsrechts der Betroffenen einhergeht.

Das derzeitige System ist inkonsequent und schützt die Persönlichkeitsrechte der Betroffenen nur unvollständig. Die Aufsichtsbehörden besitzen zwar die Kompetenz, Verfahren untersagen zu können, wenn die Datensicherheit nicht gegeben ist, andererseits sind ihnen aber bei der eindeutig gesetzeswidrigen Erhebung, Verarbeitung und Nutzung der Daten die Hände gebunden. Nach der bisher herrschenden Rechtsauffassung und -praxis bleibt den Aufsichtsbehörden letztlich nur eine repressive Vorgehensweise. Zwar können die Aufsichtsbehörden beratend tätig werden; ein Verfahren bereits im Vorfeld unterbinden können sie jedoch nicht. Dies bedeutet, dass die rechtswidrige Erhebung, Verarbeitung und Nutzung der Daten durch Aufsichtsbehörden erst hingenommen werden müssen. Nachträglich kann dann im Rahmen des Bußgeldverfahrens ein Verstoß sanktioniert werden. Die Technik und die teilweise hochkomplexe Architektur moderner Datenverarbeitung führen dazu, dass die Verbreitung von einmal in den Verkehr gebrachten Daten kaum mehr zu kontrollieren ist. Der einmalige Verstoß gegen das Recht auf informationelle Selbstbestimmung wird damit perpetuiert.

Durch die Konkretisierung des § 38 Abs. 5 BDSG könnte in diesem Bereich Klarheit geschaffen werden. Die Aufsichtsbehörden würden damit eindeutig präventive Befugnisse erlangen, um bereits im Vorfeld die Verletzung der Persönlichkeitsrechte zu verhindern, wie dies in verwandten Rechtsgebieten z.B. dem Gewerberecht, Praxis ist.

b) Erweiterung der Bußgeldtatbestände

Eines der wichtigsten Instrumente der Betroffenen zur Verfolgung ihrer verfassungsmäßigen Rechte ist das **Auskunftsrecht**. In der Vollzugspraxis der Aufsichtsbehörden zeigt sich, dass dieses Recht von vielen Daten verarbeitenden Stellen unzureichend oder gar nicht beachtet wird. Ursache dieser Missachtung der Betroffenenrechte ist u.a. die fehlende Sanktionierung des Verstoßes. Während die Nichterteilung der Auskunft gegenüber der Behörde nach § 43 Abs. 1 Nr. 10 BDSG ein Bußgeldtatbestand darstellt, wird die Nichtbeachtung des elementarsten Rechts der Betroffenen nicht sanktioniert. Die **Nichterteilung der Auskunft** durch die Daten verarbeitende Stelle gegenüber dem Betroffenen bleibt **sanktionslos**. Der Betroffene kann damit ohne Hilfe der Aufsichtsbehörden nicht erfahren, wer welche Daten zu welchem Zweck gespeichert hat. Derzeit überbrückt das ULD diese Regelungslücke, indem nach zweimaliger Aufforderung zur Stellungnahme durch den Betroffenen das ULD seinen eigenen Anspruch auf Auskunft gemäß § 38 BDSG gegenüber der Stelle geltend macht und damit auch die Interessen der Einzelnen wahrnimmt. Dies führt zu einer nicht unerheblichen Anzahl von Eingaben mit dem entsprechenden Bearbeitungsaufwand. Die Anzahl von solchen Eingaben könnte durch eine schärfere Sanktionierung der Nichtbeachtung des Auskunftsrechts verringert werden.

Gemäß § 4g Abs. 2 BDSG obliegt jeder Daten verarbeitenden Stelle die Erstellung eines Verfahrensverzeichnisses mit dem Inhalt des § 4e BDSG. Die Verletzung dieser Pflicht wird im BDSG nicht sanktioniert. Das **Verfahrensverzeichnis** ist sowohl für die Aufsichtsbehörden als auch für die Betroffenen, aber auch für die Unternehmen selbst ein Instrument, das Auskunft über den Inhalt und den Umfang der wirtschaftlichen Tätigkeit mit Bezug zur Verarbeitung personenbezogener Daten gibt. Mit wenig bürokratischem Aufwand können sich Aufsichtsbehörden unter Vorlage des Verzeichnisses einen Überblick über die Verarbeitungsprozesse innerhalb eines Unternehmens verschaffen. Außerdem wird dadurch die Transparenz für die Betroffenen erhöht. Letztlich trifft die Pflicht zur Führung eines Verfahrensverzeichnisses jedes Unternehmen, das personenbezogene Daten erhebt und verarbeitet, und stellt damit die Minimalanforderung an Unternehmen in Hinblick auf das formelle Datenschutzrecht dar. Die Nichtbefolgung der Erstellung sollte daher wie die Nichtbestellung des betrieblichen Datenschutzbeauftragten behandelt werden und mit einem Bußgeld sanktioniert werden.

§ 43 Abs. 2 Nr. 1 BDSG unterstellt nur die unzulässige Erhebung und Verarbeitung personenbezogener Daten der Sanktion mit einem Bußgeld. Die unzulässige Nutzung personenbezogener Daten wird nicht erfasst (Dammann in Simitis, Bundesdatenschutzgesetz). Aus der Gesetzesbegründung lässt sich nicht erkennen, warum z.B. die inhaltliche Auswertung rechtswidrig erlangter Daten sanktionslos bleiben soll (BT-Drs. 14/4329, 47). So ist das „Abtelefonieren“ eines Telefonbuches zu Werbezecken zwar unzulässig, kann aber nach der

derzeitigen Rechtslage nicht sanktioniert werden. Das Bundesdatenschutzgesetz ist daher in § 43 Abs. 2 Nr. 1 BDSG dahingehend zu ergänzen, dass auch die **unzulässige Nutzung personenbezogener Daten als Ordnungswidrigkeit** gewertet wird.

c) Gewinnabschöpfung

Das ULD begrüßt grundsätzlich den von BMJ Zypries und anderen politischen Akteuren gemachten Vorschlag, eine gesetzliche Regelung zu schaffen, die es erlaubt, den durch den Datenmissbrauch entstandenen Gewinn einzuziehen. In Anlehnung an § 10 UWG könnte in das BDSG eine solche Regelung aufgenommen werden. Das ULD weist jedoch darauf hin, dass gemäß § 17 Abs. 4 OWiG die Geldbuße den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen soll. Diese Vorschrift dient der Abschöpfung des rechtswidrig erlangten wirtschaftlichen Vorteils. Der **Vorteilsabzug** bildet den **Sockel der Sanktion**, auf den in der Regel die **Geldbuße aufgesetzt** wird (Bohnert, OWiG, 2. Aufl. 2007, § 17, Rdn. 25). Ob aufgrund der gesetzlichen Definition des Bußgeldzwecks und der bereits bestehenden Verfallsvorschrift des § 29a OWiG eine eigenständige Vorschrift zur Gewinnabschöpfung im BDSG zweckmäßig ist und rechtlichen Bestand hat, erscheint zweifelhaft.

d) Sanktionsrahmen

Der bisherige Sanktionsrahmen wurde in der Praxis des ULD und, soweit derzeit bekannt, auch von anderen Aufsichtsbehörden weder im Bereich des Ordnungswidrigkeitenrechts noch im Strafrecht vollständig ausgeschöpft. Dies lag vor allem daran, dass die Sanktionswürdigkeit bisher von Seiten der zuständigen Staatsanwaltschaften nicht hinreichend anerkannt wurde. Aufgrund der bekannt gewordenen datenschutzrechtswidrigen Praktiken und der damit weitergehenden Folgen für die Betroffenen ist von einer Sensibilisierung der verantwortlichen Akteure für das Schadenspotential für die Betroffenen und die Volkswirtschaft auszugehen. Es ist daher absehbar, dass die derzeitigen Sanktionsrahmen mittelfristig nicht mehr ausreichen werden. Zudem wird mit einer Erhöhung des Sanktionsrahmens die Bedeutung der Delikte zum Ausdruck gebracht. Bisher wurden Datenschutzdelikte eher als individuelle Verstöße betrachtet. Bei den in jüngster Zeit bekannt gewordenen Delikten handelt es sich zweifellos um eine besondere Form der **Wirtschafts-kriminalität**. In einer Gesellschaft, in der wirtschaftlich relevante informationstechnische Kommunikation eine zunehmende Rolle spielt, droht diese Form der Wirtschaftskriminalität immer gefährlicher zu werden und geht über die individuelle Betroffenheit Einzelner hinaus.

Die **Erhöhung des Sanktionsrahmens** sollte sich an den vergleichbaren Sanktionen bei Wirtschaftskriminalität orientieren. Formverstöße gegen das Telemediengesetz werden gemäß § 16 Abs. 3 mit Geldbußen bis zu 50.000 Euro geahndet. Der Bußgeldrahmen des Telekommunikationsgesetzes bewegt sich zwischen 10.000 und 500.000 Euro. Die Verletzung betriebsbezogener Aufsichtspflichten hingegen kann gemäß § 130 Abs. 3 OWiG eine Geldbuße von bis zu 1 Million Euro nach sich ziehen.

Es wird daher seitens des ULD vorgeschlagen, die Höhe des Bußgeldes für Verstöße gegen das formelle Datenschutzrecht (§ 43 Abs. 1 BDSG) auf 50.000 Euro und Verstöße gegen das materielle Datenschutzrecht (§ 43 Abs. 2 BDSG) auf 500.000 Euro zu erhöhen. Außerdem sollte § 43 Abs. 2 BDSG klarstellen, dass im Einzelfall, nämlich dann, wenn das Bußgeld den aus der Ordnungswidrigkeit gezogenen wirtschaftlichen Vorteil nicht übersteigt, die genannten Betragsgrenzen überschritten werden können (vgl. dazu § 149 Abs. 2 TKG).

e) Antragsrecht der Aufsichtsbehörden im Bereich des StGB

Häufig werden den Aufsichtsbehörden Datenschutzverstöße, die den Kernbereich der privaten Lebensgestaltung treffen, zur Kenntnis gegeben. Die Schwerpunkte dieser Verstöße liegen dann in der Regel nicht in der Erhebung, Verarbeitung oder Nutzung von Daten. Die Aufsichtsbehörden sind daher für die Verfolgung und Sanktionierung nicht zuständig. Zu diesen Verstößen gehören vor allem Straftaten die in den §§ 201-204 StGB (Verletzung des persönlichen Lebens- und Geheimbereichs) normiert sind. Diese Delikte zählen jedoch gemäß § 205 StGB zu den **absoluten Antragsdelikten**. Sie werden daher nur auf einen entsprechenden Strafantrag der Verletzten durch die Staatsanwaltschaften und Gerichte verfolgt.

Gerade bei der Verletzung von Rechten innerhalb von Arbeitsverhältnissen (Ton- und exzessive Videoüberwachung) und sonstigen Garantenverhältnissen (Arzt und Patient, Anwalt und Mandant) sind die Betroffenen aufgrund der bestehenden wirtschaftlichen Abhängigkeit oder des besonderen Vertrauensverhältnisses zurückhaltend oder nicht bereit, den erforderlichen Strafantrag zu stellen. Das Fehlen des Strafantrages stellt aber ein absolutes Verfolgungshindernis dar.

Würden die **Aufsichtsbehörden** diesbezüglich ein **Antragsrecht** erhalten, wäre eine effektivere Durchsetzung der Schutzgüter möglich. Denn die Rechtsverletzungen berühren nicht nur hochpersönliche Rechte der Betroffenen. So ist das Vertrauen in die Wahrung der Vertraulichkeit des nichtöffentlich gesprochenen Wortes, des Schutzes des höchstpersönlichen Lebensbereiches vor Ausspähung oder des Schutzes von Privatgeheimnissen durch besondere Berufsgruppen auch eine gesamtgesellschaftliche Frage, denn die Selbstbestimmung des Einzelnen ist „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens“ (BVerfG, Urteil vom 15.12.1983 – 1 BvR

209/83 u.a., NJW 1984, 419, 423). Alternativ – oder zusätzlich – wäre eine Ergänzung des § 205 StGB dahin gehend denkbar, dass die **Staatsanwaltschaft** bei der Feststellung eines öffentlichen Interesses an der Verfolgung der Tat das Fehlen des Strafantrages als Verfolgungshindernis überwinden kann.

f) Informationspflichten gegenüber den Betroffenen bei Datenschutzpannen und -verstößen

Die Informationspflicht von Betroffenen bei Datenschutzpannen und -verstößen („breach notification") hat seinen Ursprung in den USA und fand Eingang in den von der EU-Kommission gemachten Vorschlag zur Revision der Telekommunikations-Datenschutzrichtlinie (ePrivacy Directive). Dieser Vorschlag wird u.a. unterstützt von BMELV Seehofer und BMJ Zypries. Die Erfahrungen aus der Prüfungspraxis des ULD zeigen, dass Unternehmen häufig noch vor der Sanktion des Bußgeldes die Information der Betroffenen bei einer Verletzung als Sanktionsmaßnahme fürchten. Dies gilt umso mehr in Branchen, in denen die Vertrauensbeziehung zwischen Betroffenen und Unternehmen als eines der Wettbewerbsvorteile vor Marktkonkurrenten angesehen wird, z.B. in der Versicherungs-, Finanz- und Kreditwirtschaft.

Die **Informationspflicht** muss dabei gestuft aufgebaut sein. In Abhängigkeit vom Umfang des Verstoßes wären Unternehmen verpflichtet, zuerst die Betroffenen individuell zu informieren. Ist die Individualinformation nicht praktikabel oder unverhältnismäßig, wäre die öffentliche Bekanntmachung z.B. gegenüber den Medien einzuführen. Zusätzlich sind die zuständigen Datenschutzaufsichtsbehörden zu informieren.

Der Inhalt der Information sollte eine standardisierte Form haben und

- den Betroffenen über die Existenz des Verstoßes und den Zeitpunkt informieren,
- mitteilen, welche Daten bzw. Datenkategorien in welcher Form von dem Verstoß erfasst sind oder waren,
- bekanntgeben, welche Maßnahmen ergriffen wurden, um den Verstoß zu beenden bzw. Schaden zu mindern, und
- welche Rechte der Betroffene gegenüber der verantwortlichen Stelle besitzt sowie die Maßnahmen benennen, durch die Betroffenen selbst zur Minimierung des Schadens beitragen können.

Entsprechende Meldungen könnten in einem zentralisierten Register vorgehalten werden. Mittelfristig sollte die Errichtung eines europäischen Zentralregisters angestrebt werden, das im automatisierten Abrufverfahren zugänglich ist.

g) Schadenersatz für immateriellen Schaden

Bisher ist der Schadensersatz in § 7 BDSG nur für materielle Schäden geregelt. Zu fordern ist hier eine Regelung, die ausdrücklich immaterielle Schäden in den Ersatzanspruch aufnimmt. In den meisten Fällen entstehen die Betroffenen keine gerichtsfest nachweisbaren materiellen Schäden. Die erfolgte **Rufschädigung, Stigmatisierung oder Belästigung** der Betroffenen durch unzulässige Datenverarbeitung z.B. im Rahmen von Werbeanrufen lassen sich kaum in konkreten Beträgen darstellen. Selbst wenn dies aufgrund von Anwaltskosten etc. möglich ist, spiegeln sie nicht die tatsächliche Verletzung des Persönlichkeitsrechts der Betroffenen wider. Die konkrete Verankerung des immateriellen Schadens würde auch zu einer Entlastung der Tätigkeit der Aufsichtsbehörden führen. Diese könnten dann häufiger auf den Privatrechtsweg verweisen, der somit größere Aussicht auf Erfolg versprechen würde.

3. Materiellrechtliche Änderungen

a) Opt-in bei Nutzung von Daten für Werbezwecke

Eine seit Jahren von den Aufsichtsbehörden geforderte Änderung des Gesetzes betrifft die Weitergabe von personenbezogenen Daten für Werbezwecke. Diese muss generell unter den Einwilligungsvorbehalt der Betroffenen gestellt werden. Die Weitergabe personenbezogener Daten muss von der **informierten Einwilligung** der Betroffenen (§ 4a BDSG) abhängig sein. Die bisherige Privilegierung der Werbenutzung ist verfassungsrechtlich fragwürdig (vgl. Weichert in Taeger/Wiebe, Informatik-Wirtschaft-Recht, Festschrift für Kilian, 2004, 295) und rechtspolitisch anachronistisch. Die Erfahrungen mit den bisherigen Regelungen ist, dass sie zu weit sind und in der Praxis nicht beachtet werden (dies gilt für die Abwägungsklausel in § 28 Abs. 1 Nr. 2 BDSG und in großem Umfang für die Hinweispflichten und Widerspruchsrechte in § 28 Abs. 4 BDSG).

b) Koppelungsverbot

Firmen muss untersagt werden, dass diese die Zustimmung zur übermäßigen Datennutzung zur Bedingung für den Vertragsabschluss machen. Ein derartiges Verbot gibt es bisher nur im Telemedienrecht (§ 12 Abs. 3 TMG). Da aber das Abfordern von Daten, die für die Vertragsabwicklung nicht benötigt werden, sich nicht auf diese Branche beschränkt, ist das Koppelungsverbot auch im BDSG zu verankern.

c) Inhalt des Auskunftsrechts

Das Auskunftsrecht nach § 34 BDSG erfasst derzeit nicht die Information über die Herkunft der Daten, soweit diese nicht von den Unternehmen mitgespeichert wird. Dies ist in der Regel bei den verantwortlichen Stellen nicht der Fall. Die **Auskunftspflicht auf Herkunft oder Ursprung der Daten zu erstrecken**, würde den illegalen Datenhandel erschweren bzw. stark reduzieren. Die Schließung dieser Regelungslücke sollte mit der Pflicht zur Speicherung der **Herkunftskette** (ggf. technisch abgesichert mit Hilfe von digitalen Signaturen) begleitet werden. Dadurch wäre der Betroffene nicht darauf angewiesen, selber dem Verlauf der Übermittlung zu folgen, sondern die verantwortliche Stelle müsste die Rechtmäßigkeit der Übermittlung gegenüber dem Betroffenen nachweisen bzw. nachvollziehbar machen. Denn die jeweiligen Unternehmen wären verpflichtet, die Erhebung und Quelle zu dokumentieren.

Damit wird der Druck erhöht, datenschutzkonform Daten zu erheben, weil durch die Nachverfolgbarkeit der Datenfluss transparent wird und rechtswidrige Erhebungspraxen nicht mehr verdeckt werden können. Zwar besteht die Pflicht zur Information bei der erstmaligen Speicherung gemäß § 33 Abs. 1 BDSG, jedoch wird diese Verpflichtung regelmäßig durch die Unternehmen missachtet, da der Vorgang der Übermittlung aus der Natur der Sache heraus durch die Betroffenen nicht wahrgenommen werden kann. Betroffene sind daher auf die Mitwirkung der Unternehmen angewiesen, ohne diese selbst effektiv kontrollieren zu können. Wie bereits angesprochen, sollte diese Maßnahme durch eine Pönalisierung der Nichterteilung der Auskunft gegenüber dem Betroffenen begleitet werden. Dies würde die Rechte der Betroffenen stärken und zu einer Entlastung der Aufsichtsbehörden führen.

d) Technische und organisatorische Maßnahmen

Eine massive rechtliche Verbesserung würde auf dem gesamten Gebiet des Datenschutzes im nichtöffentlichen Bereich erreicht, wenn die Ziele der technische und organisatorischen Maßnahmen – wie in vielen Landesdatenschutzgesetzen (LDSG) – auch ausdrücklich in das BDSG aufgenommen würden: **Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit sowie Transparenz**. Damit würde zugleich eine Konkretisierung des jüngst vom Bundesverfassungsgericht (BVerfG) geschaffenen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfolgen (U.v. 27.02.2008, Az. 1 BvR 370/07 u.a.). Zur Gewährleistung der Revisionsfähigkeit ist beispielsweise eine grundsätzliche Pflicht zur Protokollierung von Zugriffen auf personenbezogene Daten durch Unternehmen wünschenswert. Auch die Wahrnehmung der Betroffenenrechte sollte stärker technisch unterstützt werden, indem im Unternehmen Datenschutzmanagementsysteme eingesetzt werden und Auskunftsersuchen von Betroffenen durch den Einsatz technischer Verfahren erleichtert werden.

4. Grundsätzliche Erwägung zum Verhältnis Datenschutz und Verbraucherschutz

Bisher wird von den Gerichten in Frage gestellt, dass es sich beim Datenschutzrecht um verbraucherschützende Normen handelt, die auch von den Verbraucherzentralen gerichtlich durchgesetzt werden könnten (dazu Weichert VuR 2006, 377, siehe auch 452). Obwohl diese Rechtsprechung schon nach derzeitiger Gesetzeslage kaum haltbar ist, wäre es im Interesse einer klaren Aufgabenzuordnung und der Rechtssicherheit geboten, gesetzlich klarzustellen, dass den Verbänden auch eine **Verbraucherdaten schützende Funktion** zukommt.

5. Sonstige datenschutzpolitische Forderungen

a) Verbesserung der Datenschutzkontrolle

Derzeit sind die Aufsichtsbehörden nach § 38 BDSG personell und sachlich so ausgestattet, dass diese ihre Aufgaben nicht ansatzweise befriedigend erfüllen können. Es gibt – soweit bekannt – derzeit kein Bundesland, in dem eine zweistellige Zahl von Personen für die Datenschutzaufsicht im Privatbereich eingesetzt wird. Der Umstand, dass diese öffentlich Bediensteten zumeist mehrere 100.000 Betriebe überprüfen sollen, erklärt u.a. die bestehenden Vollzugsdefizite. Hier ist ein Ausbau der personellen Kapazitäten geboten.

b) Umsetzung des § 9a BDSG: Datenschutzaudit

Der Begriff „Datenschutzaudit" umfasst sowohl Produkt- als auch Verfahrensevaluationen. Da damit jeweils unterschiedliche Anforderungen an die Prozesse der Evaluation und Zertifizierung verbunden sind, sollte nach Produktaudit („Datenschutz-Gütesiegel") und Verfahrensaudit unterschieden werden. Aus den Zertifikaten muss hervorgehen, um welche Art des Datenschutzaudits es sich handelt.

Zur Erreichung einer möglichst hohen Akzeptanz der freiwilligen Verfahren ist eine Umsetzung entsprechend der anerkannten Audit-Standards ISO/IEC 19011:2002 („Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen") geboten.