Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
www.datenschutzzentrum.de/

Stellungnahme des ULD
zum Gesetzentwurf des Bundesministerium des Innern - Referentenentwurf
Stand 13.10.2008

Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits

hier Art. 2 - Datenschutzauditgesetz (DSAG-E)

I. Allgemeine Bemerkungen

Das Vorhaben, ein Datenschutzauditgesetz auf den Weg zu bringen, ist angesichts des seit dem Jahr 2001 bestehenden Gesetzesauftrags des § 9a BDSG (Bundesdatenschutzgesetz) und des hohen und weiter **steigenden Bedarfs** an einem gesetzlich geregelten präventiven Instrument zur Bestätigung der Datenschutzkonformität von Produkten, Dienstleistungen und Verfahren sehr zu begrüßen.

Beim sog. Datenschutzgipfel am 4. September 2008 hat das Bundesministerium des Innern in Reaktion auf das Bekanntwerden des illegalen Handels mit sensiblen Personendaten, insbesondere Kontodaten, die Grundzüge des vorliegenden Gesetzentwurfes angekündigt. Dies wurde umgehend vom Leiter des ULD mit dem Hinweis kommentiert, dass die dargelegte Konzeption eine Vielzahl von praktischen Probleme verursachen werde, die vermeidbar sind. Er hat seine **Beratung angeboten**. Das ULD ist die einzige öffentliche Stelle in Deutschland, die - seit über 7 Jahren - praktische Erfahrungen mit der Verleihung von Datenschutzgütesiegeln und der Durchführung von Datenschutzauditverfahren hat. Der Leiter des ULD hat beim Gipfel weiterhin darauf hingewiesen, dass die europäischen Koordinierungsbestrebungen, die im Rahmen des von der Europäischen Kommission geförderten Projektes European Privacy Seal (EuroPriSe), an dem sich 9 Stellen aus 8 EU-Mitgliedsstaaten beteiligen, berücksichtigt werden sollten. Mit Schreiben vom 14.10.2008 hat das ULD gegenüber dem Bundesministerium des Innern (BMI) seine Bereitschaft zur Beratung schriftlich erneuert. Eine Reaktion auf diese Angebote ist bisher nicht erfolgt. Leider lässt sich dem vorliegenden Gesetzentwurf (DSAG-E) auch nicht entnehmen, dass irgendwelche praktischen Erfahrungen aus der Datenschutzauditierung eingeflossen wären. EuroPriSe wird selbst in der Gesetzesbegründung überhaupt nicht zur Kenntnis genommen.

Der DSAG-E basiert auf der Gesetzgebungskompetenz des Bundes für das Recht der Wirtschaft (Art. 72 Abs. 2, 74 Ans. 1 Nr. 11 GG). Im Interesse einer bundesweiten einheitlichen Regelung ist dies zu begrüßen. Die **Zuständigkeit** für die Erfüllung staatlicher Aufgaben liegt nach Art. 30 GG grundsätzlich bei den Ländern. Für die vorgesehenen Zuständigkeiten auf Bundesebene gibt es weitgehend keine sachliche Notwendigkeit und damit auch keine Rechtfertigung.

Adressat des DSAG sollen ausschließlich Stellen sein, die zueinander im Wettbewerb stehen, also v.a. nicht-öffentliche Stellen (§ 1 S. 1, 3 DSAG-E). Für öffentliche Stellen der Länder besteht auf Landesebene die Möglichkeit spezifischer Regelungen. Hiervon haben bisher die Länder Bremen und Schleswig-Holstein Gebrauch gemacht. **Öffentliche Stellen des Bundes** sollen gemäß dem Entwurf i.d.R. von Datenschutzaudits nicht profitieren können. Dies wird damit begründet, dass es für die erhöhte Akzeptanz der Bürgerinnen und Bürger bei der Inanspruchnahme einer E-Government-Anwendung "ausreichend" sei, "dass mit einem Datenschutzauditsiegel gekennzeichnete Datenschutzkonzepte und technische Einrichtungen eingesetzt werden können" (Begr. S. 16). Dies widerspricht den Erfahrungen von teilweise sehr umfassenden Datenschutzaudits in Kommunen und bei der Landesverwaltung in Schleswig-Holstein. Bei den bisher seit 2001 durchgeführten 23 Verfahrensaudits nach § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) war es möglich, auf äußerst effektive Weise teilweise gravierende Mängel insbesondere bei der Datensicherheit und beim Datenschutzmanagement zu beheben. Die öffentlichen

Stellen in Schleswig-Holstein nehmen das Angebot im Rahmen der zur Verfügung stehenden Kapazitäten umfassend in Anspruch. Es haben sich auch schon öffentliche Stellen des Bundes an das ULD mit der Bitte gewandt, ein gebührenpflichtiges Audit durchzuführen. Ein derartiges rechtsförmliches Audit war dem ULD wegen der Rechtslage nicht möglich. Es ist kein Grund ersichtlich, weshalb den öffentlichen Stellen des Bundes diese Chance vorenthalten werden soll.

Gegenstand des Datenschutzaudits sollen Datenschutzkonzepte sowie technische Einrichtungen sein. Deren Umfang soll durch das beantragende Unternehmen festgelegt werden. Anders als in Schleswig-Holstein geht der BDSAG-E nicht auf die Unterschiede der **Zertifizierung von Produkten und Dienstleistungen** einerseits (Datenschutzgütesiegel nach § 4 Abs. 2 LDSG SH) und der **Auditierung von Stellen, Organisationseinheiten oder Verfahren** ein. Diese vom DSAG-E nicht nachvollzogene Differenzierung ist nicht zwingend. Das im DSAG-E vorgeschlagene Verfahren ist aber nicht ansatzweise für die Zertifizierung von Produkten geeignet. Dies zeigt sich schon an § 1 S. 2 DSAG-E, wo z.B. die Anforderung der Nr. 3 (Beachtung der Normen zum betrieblichen Datenschutzbeauftragten) für die Qualität von IT-Produkten regelmäßig überhaupt keine Relevanz hat, so wichtig und sinnvoll es auch ist, dass sowohl bei der Entwicklung von Produkten wie auch bei deren Einsatz eine Einbeziehung des betrieblichen Datenschutzbeauftragten erfolgt. Bei Produkten kommt es darauf an, dass sich deren Nutzer zum Zeitpunkt der Entscheidung der Anschaffung darauf weitgehend verlassen können müssen, dass diese gesetzeskonform eingesetzt werden können. Während bei umfassenden, in der Regel schon im Betrieb befindlichen Verfahren eine Nachbesserung bei auftretenden Mängeln nachträglich möglich ist, ist dies bei Produkten oft nicht oder nur sehr schwer machbar. In der verlässlichen hoheitlichen Bestätigung der Rechtskonformität sehen Produktanbieter den wesentlichen Wettbewerbsvorteil der vom ULD mit einem Gütesiegel ausgezeichneten Produkte. Diese Chance wird relativiert bzw. vertan, wenn nicht eine vertrauenswürdige, unabhängige öffentliche Stelle die Datenschutzkonformität vorab feststellt. Vertrauen wird nicht durch das Siegel selbst geschaffen, sondern ausschließlich durch die Vertrauenswürdigkeit der das Siegel verleihenden Einrichtung und des Auditverfahrens. Gegenüber dem schleswig-holsteinischen Gütesiegel entfällt bei dem nach dem DSAG-E gewählten Verfahren zudem der Wettbewerbsvorteil, dass bei öffentlichen Beschaffungen zertifizierte Produkte vorrangig zu berücksichtigen sind (§ 4 Abs. 2 LDSG SH).

Bei Produkten ist es grundsätzlich sinnvoll und wünschenswert, eine Zertifizierung auch vornehmen zu können, wenn die Produkte nicht von Stellen in Deutschland hergestellt bzw. vemarktet werden. Eine Vielzahl von **ausländischen IT-Produkten und Dienstleistungen** wird angesichts der Globalisierung der Informationstechnik auf dem deutschen Markt angeboten. Es ist nicht ersichtlich, weshalb diese IT-Produkte und Dienstleistungen von den Vorteilen einer Auditierung nicht profitieren können sollen. So hat z.B. das Unternehmen Microsoft aus Redmond/USA zur Verbesserung seiner Wettbewerbschancen auf dem europäischen Markt schon zwei seiner Produkte in Schleswig-Holstein zertifizieren lassen. Es ist zudem fraglich, ob die Beschränkung auf deutsche Anbieter (§ 1 Abs. 1 S. 1) mit europäischem Recht vereinbar ist.

Der DSAG-E sieht vor, dass eine Auditierung nur dann erfolgen soll, wenn über die gesetzlichen Anforderungen hinaus Verbesserungen für den Datenschutz implementiert sind (Begr. S. 16). Dies ist ein zweifellos ehrgeiziges Anliegen. Dieses Ziel wird aber nicht erreicht, wenn selbst **bei festgestellten Datenschutzverstößen** von mittlerer Bedeutung das Siegel beibehalten werden kann (§ 6 Abs. 2 S. 1).

Der Entwurf legt nicht fest, welches Maß der **Übererfüllung der rechtlichen Anforderungen** notwendig ist. Gerade bei Produkten wäre es für den Datenschutz schon ein großer Gewinn, wenn deren rechtmäßige Einsatzmöglichkeit bestätigt würde. Die Entwurfsautoren gehen fälschlich davon aus, dass die Einhaltung der Datenschutzgesetze die Regel wäre. Dies liegt nicht am bösen Willen oder gar an der kriminellen Absicht der Anwender. Es gibt viele Produkte, die teilweise eine Marktabdeckung von mehr als 50% in einem bestimmten Segment in Deutschland haben, die auf Grund der technischen Gegebenheiten nicht rechtskonform eingesetzt werden können (z.B. wegen fehlender oder mangelhafter Protokollierung, mangels der Möglichkeit einer Einzeldatenlöschung, wegen fehlender Einwilligungswahlmöglichkeit für den Betroffenen, auf Grund der Einbeziehung von Übermittlungen ins Drittausland). Wegen oft fehlender eigener hinreichender technischer und rechtlicher Kompetenz kommt es dem Erwerber eines IT-Produktes v.a.

darauf an, sich zu vergewissern, dass er mit dessen regulärem Einsatz "auf der sicheren Seite" ist. Auch ein sich auf Gesetzeskonformität beschränkendes Datenschutzauditsiegel würde nicht Gefahr laufen, die darüber hinausgehenden Kontrollen von Datenschutzaufsichtsbehörden zu entwerten oder gar einen faktischen Zwang zur Auditierung auszulösen. Die dies behauptende Passage der Begründung (S. 17) zeigt, dass die Autoren des DSAG-E die Besonderheit der Datenschutzzertifizierung nicht vollständig erfasst haben: Während bei der Zertifizierung "auf dem Gebiet des ökologischen Landbaus", die als Vorbild herangezogen wurde (Begr. S. 18), die Einhaltung von klaren rechtlichen Anforderungen (Grenzwerte, überschaubare Produktpalette und einfache Abläufe) von den Aufsichtsbehörden relativ einfach festgestellt werden kann, hängt die Datenschutzkonformität des Einsatzes eines IT-Produktes nicht nur von diesem selbst ab, sondern von den gegebenen technischen und organisatorischen Rahmenbedingungen, von den Schnittstellen zu angeschlossenen Verfahren und v.a. von der konkreten Nutzung durch die Anwender, d.h. von Organisationen und ihren Beschäftigten. Mit einem Audit kann und soll die Voraussetzung dafür geschaffen werden, dass ein rechtskonformer Einsatz möglich und erleichtert wird. Die tatsächliche Beachtung der Datenschutzgesetze, deren Kontrolle den Aufsichtsbehörden obliegt, ist ein weit über die Zertifizierung hinausgehendes Feld.

Der Grundansatz des DSAG-E, der abweicht von allen in diesem Bereich üblichen staatlich geregelten Zertifizierungen, besteht darin, die Auditierung durch private Stellen (sog. Kontrollstellen) vornehmen zu lassen. Dem gegenüber sieht z.B. die Zertifizierung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) oder des ULD eine **Qualitätssicherung** der von privaten Gutachtern durchgeführten Audits vor. Diese Qualitätssicherung ist dringend notwendig, um Billig- und Gefälligkeitszertifikate auszuschließen. Anders als etwa im Bereich des Umweltschutzes oder des biologischen Landbaus sind die datenschutzrechtlichen und -technischen Anforderungen hoch komplex, von Produkt und Verfahren zu Produkt und Verfahren unterschiedlich und in einer dauernden Fortentwicklung. Die Erfahrungen des ULD zeigen, dass selbst engagierten und qualifizierten privaten Gutachtern aktuelle Anforderungen oft nicht bekannt und bewusst waren bzw. sind. Diese Anforderungen lassen sich auch nicht durch ein schwerfälliges Verfahren in einem Datenschutzauditausschuss (§ 13 DSAG-E) festlegen, sondern ergeben sich oft aus technologischen Neuentwicklungen und der aktuellen Forschung. Im Dialog zwischen Gutachtern und Zertifizierungsstelle war es in Schleswig-Holstein bisher möglich, einen Konsens über die rechtlich geforderte Qualität des Produktes, der Dokumentation und des Gutachtens herzustellen. Hierbei hat es sich als vorteilhaft erwiesen, dass auf die Kontroll- und Beratungserfahrung einer Aufsichtsbehörde nach § 38 BDSG zurückgegriffen werden konnte, die im Diskussionszusammenhang mit den anderen Aufsichtsbehörden (sog. Düsseldorfer Kreis) bzw. Datenschutzbeauftragten (Konferenz der Datenschutzbeauftragten des Bundes und der Länder) steht. Die Qualitätssicherung liegt nicht nur im Interesse der Produktanbieter und der Produktkäufer, sondern auch der Gutachter, die vor Abgabe des endgültigen Gutachtens oft auf einen Dialog mit der Zertifizierungsstelle angewiesen sind, um Fehlbeurteilungen zu vermeiden.

Ein zentraler Aspekt der Qualitätssicherung besteht darin, dass alle interessierten Personen und Stellen die Berechtigung des Zertifikats überprüfen können. Dies gilt insbesondere für den Datenschutz und die Datensicherheit, die beide wegen ihrer dauernden Weiterentwicklung und Komplexität, auch durch Wechselwirkungen mit anderen Funktionalitäten, weder von Gutachtern noch von Aufsichtsbehörden abschließend beurteilt werden können. Daher kommt der **Transparenz gegenüber der Öffentlichkeit** eine zentrale Bedeutung für die Qualität und Vertrauenswürdigkeit des Zertifikats zu. Diese beginnt mit einer präzisen Beschreibung des Auditierungsgegenstands, um keine falschen Vorstellungen vom Umfang der Zertifizierung entstehen zu lassen. Beschrieben werden müssen alle wesentlichen Eigenschaften, Abläufe, Schnittstellen, Einsatzbedingungen und Sicherheitsvorkehrungen. Nur wenn das Audit auch qualifiziert öffentlich in Frage gestellt werden kann, findet es die nötige allgemeine Akzeptanz. Dies setzt nicht voraus, dass die zum Einsatz kommenden Algorithmen, Quellcodes oder Betriebs- und Geschäftsgeheimnisse offengelegt werden müssten. Wohl aber ist es nötig, die wesentlichen Funktionsweisen plausibel und nachvollziehbar darzustellen. Dies begründet bei Betroffenen und Anwendern das notwendige Vertrauen, bei kritischer Öffentlichkeit und Aufsichtsbehörden den Ansatz zur Überprüfung, und bei Gutachtern und Anbietern das nötige Feedback auf Auftreten von Angriffsmöglichkeiten. Bei den in Schleswig-Holstein

durchgeführten Auditierungen wird die Transparenz dadurch hergestellt, dass die Kurzgutachten im Internet allgemein bereitgestellt bzw. veröffentlicht werden. Eine entsprechende Transparenz ist im DSAG-E überhaupt nicht angelegt. Die Veröffentlichung soll sich auf "das angezeigte Datenschutzkonzept sowie die technische Einrichtung" beschränken (§ 8 Abs. 2 S. 3 Nr. 3 u. S. 4). Eine Dokumentation der Erkenntnisse der Kontrolle durch die Kontrollstelle erfolgt nicht, sondern lediglich die nicht näher überprüfbare Erklärung der Kontrollstelle, bei welchen Stellen Kontrollen durchgeführt wurden (§ 5 Abs. 2).

Es drängt sich der Eindruck auf, dass der DSAG-E nicht darauf abzielt, eine vertrauenswürdige präventive Datenschutzüberprüfung durchzuführen, sondern darauf, die staatliche **Aufsicht durch eine nachträgliche private Kontrolle zu ersetzen**. Mit dem Gesetz würde die Verantwortlichkeit für die Rechtmäßigkeit der Datenverarbeitung von der kontrollierten Stelle zu einem Teil auf die Kontrollstelle übertragen, aber auch die Verantwortlichkeit für die Datenschutzkontrolle durch die Aufsichtsbehörde würde teilweise auf die Kontrollstelle übertragen. Die Kontrollstelle kommt ihren daraus sich ergebenden Pflichten dadurch förmlich nach, dass sie gegenüber den Aufsichtsbehörden bestätigt und sich verpflichtet, Kontrollen nach § 3 durchzuführen. Qualifiziertere Feststellungen werden grds. von der Kontrollstelle nicht abverlangt (§ 5 Abs. 2). Das Konzept würde dazu führen, dass bei der Feststellung von Verstößen die Verantwortung jeweils auf eine andere Stelle abgeschoben werden kann. Tatsächliche Anreize zu einer ernsthaften Kontrolle werden nicht gegeben und würden erst dann entstehen, wenn Verstöße öffentlich bekannt würden. Damit würde keine Verbesserung des Datenschutzes, sondern eine Verschlechterung gegenüber dem aktuellen Zustand erreicht.

Die faktische Entbindung von staatlicher Kontrolle durch das DSAG ist wohl nicht mit Art. 28 Abs. 3 S. 1 3. Sp. der **Europäischen Datenschutzrichtlinie** (EU-DSRL) vereinbar, wonach "jede Kontrollstelle" über "wirksame Einwirkungsbefugnisse" verfügen muss. Der Entzug von Kontrollkompetenz durch den DSAG-E gegenüber Aufsichtsbehörden durch die zumindest anscheinende Privilegierung der kontrollierten Stellen (z.B. § 19) und die Festlegung von rechtsinterpretierenden Richtlinien durch den Datenschutzauditausschuss unter der Rechtsaufsicht des Bundesministeriums des Innern (BMI) verletzt zudem tendenziell die von Art. 28 Abs. 1 S. 2 EU-DSRL geforderte Unabhängigkeit von Kontrollstellen (auch der Länder).

Das Problem der mangelnden Qualitätssicherung versucht der DSAG-E durch ein **kompliziertes nachträgliches Kontrollverfahren** zu kompensieren. Damit wird aber die Idee des Datenschutzaudits als präventives Instrument ad absurdum geführt, weil dessen Validität von der Repression, also der aufsichtsbehördlichen Kontrolle und der Sanktionierung von Verstößen abhängig gemacht wird. Angesichts der schlechten personellen und sonstigen Ausstattung der Aufsichtsbehörden ist faktisch nicht ansatzweise die notwendige nachträgliche Qualitätssicherung gewährleistet. Dem versucht der DSAG-E offensichtlich dadurch Rechnung zu tragen, dass er die Möglichkeit einräumt, private Stellen mit den Aufsichtsaufgaben zu beleihen (§ 16 Abs. 1, 2). Da aber auch diese Tätigkeit beaufsichtigt werden muss, diese jedoch noch weniger transparent ist als die staatliche Aufsichtstätigkeit, entsteht weder ein Effekt der Entlastung von Behörden noch der einer verbesserten Kontrolle. Vielmehr werden alle Beteiligten über die Wertigkeit des konkreten Zertifikats bis zu dem Zeitpunkt im Ungewissen gehalten, zu dem über eine aufwändige Prozedur das Zertifikat wegen übermäßiger Datenschutzverstöße aufgehoben wird.

Das konzeptionelle Defizit des vom DSAG-E vorgesehenen Audits besteht darin, dass die Zertifizierung nicht durch eine **unabhängige Stelle** erfolgt. Zwar kann durch das Zulassungsverfahren eine hinreichende Qualifizierung, finanzielle Unabhängigkeit und Zuverlässigkeit sichergestellt werden (§ 4 DSAG-E). Dies ändert aber nichts an dem Umstand, dass sowohl die Kontrollstelle als auch die nicht-öffentliche Stelle ein gemeinsames Interesse haben, möglichst ohne großen Aufwand und Kosten ein Zertifikat zu führen. Um die Parteilichkeit der Auditierung zu verhindern, muss - zumindest bei der Zertifizierung von Produkten - eine ökonomisch nicht interessierte Stelle schon im Auditverfahren einbezogen werden.

Während der Entwurf eines DSAG von September 2007 offensichtlich noch davon ausging (Referententwurf des BMI vom 07.09.2007; dazu Stellungnahme des ULD vom 28.09.2007: https://www.datenschutzzentrum.de/bdsauditg/20070928-stellungnahme.html), dass die Zertifizierung ein

von Beliehenen erlassener Verwaltungsakt ist, geht der aktuelle DSAG-E davon aus, dass es sich bei der Auditierung nicht um ein Verwaltungsverfahren, sondern um ein rein **privatrechtliches Geschäft** handelt (§ 3 S. 1).

Die Formulierung des Gesetzentwurfes ist **unstrukturiert und zusammengestückelt**. So werden z.B. die materiellen Anforderungen an ein Audit in § 1 S. 2 aufgeführt; in § 8 Abs. 2 wird dann jedoch geregelt, dass eine ausdrückliche Feststellung dieser Anforderungen gar nicht nötig ist. Die Anforderungen an Kontrollstellen sind in § 4 geregelt und werden dann unvermittelt in § 9 wieder aufgegriffen. Der Entwurf verwendet eine eigene Terminologie, die sich weder aus bisherigen Gesetzen noch aus dem allgemeinen Sprachgebrauch erschließt. Dies führt dazu, dass der Inhalt des Gesetzes nur erfasst werden kann, wenn dieses insgesamt und intensiv studiert wird.

Für Betroffene dürfte das Gesetz regelmäßig zu kompliziert und unverständlich sein. Schon aus diesem Grund ist der DSAG-E nicht geeignet, bei **Betroffenen** Vertrauen in die Qualität der Audits zu fördern. Den Betroffenen wird in dem Entwurf keine aktive Rolle zugewiesen. Sie haben nicht einmal die Möglichkeit, sich über die Qualitätsmerkmale der auditierten Stelle bzw. des Auditgegenstands zu informieren und dies auf ihren Realitätsgehalt hin zu überprüfen.

Die Durchführung des Datenschutzaudits soll **freiwillig** sein (Begr. S. 15). Dies würde es notwendig machen, dass positive Marktanreize für eine solche Durchführung geschaffen würden. Davon kann beim DSAG-E aber keine Rede sein. Vielmehr entstehen neben deN Kosten- und Gebührenpflichten für das Unternehmen weitgehende zusätzliche Unterrichtungspflichten (§ 7) sowie zusätzliche Sanktionsandrohungen (§§ 17, 18).

II. Zu den spezifischen Regelungen

Zu § 1 - Datenschutzaudit

Die Beschreibung des **Auditierungsgegenstands** (Target of Evaluation - ToE) als "Datenschutzkonzept und ihre technische Einrichtung" nach Abs. 1 ist zu eng. Die Datenschutzkonformität von Produkten und Verfahren kann oft nur über die Beschreibung der Datenflüsse, der Organisation und/oder von internen Normen hergestellt werden hergestellt werden, was mit der verwendeten Terminologie begrifflich nicht erfasst wird. Daher wird empfohlen, entweder umfassend von "Produkten und Verfahren" zu sprechen oder präziser von "Produkten, Dienstleistungen, Datenverarbeitungskonzepten und Verfahren".

Die Beschränkung auf **nicht-öffentliche Stellen** i.S.d. § 2 Abs. 4 BDSG ist - wie oben dargestellt - zu eng. Erfasst werden sollten auch öffentliche Stellen des Bundes sowie ausländische Stellen. Dies lässt dadurch kurz und knapp beschreiben, dass keinerlei Einschränkung bzgl. der Anwendung erfolgt außer den nicht erfassten "öffentlichen Stellen eines Landes".

Zur zusätzlichen Anforderung in "Richtlinien zur **Verbesserung des Datenschutzes** und der Datensicherheit" siehe oben (I.) sowie die Ausführungen zu § 11.

Die in S. 2 Nr. 3 vorgesehene Beschränkung der Organisationskontrolle auf den "Beauftragten für den Datenschutz" ist zu eng. Bei einem Verfahrensaudit muss zur organisatorischen Gewährleistung des Datenschutzes ein den betrieblichen Datenschutzbeauftragten einbeziehendes, aber sich nicht hierauf beschränkendes funktionierendes, umfassendes **Datenschutzmanagement** etabliert sein (vgl. Nr. 7 der Anwendungsbestimmungen des ULD zur Durchführung eines Datenschutzbehördenaudits nach § 43 Abs. 2 LDSG SH).

Nach S. 1 Nr. 4 ist die Datenschutzkonformität **regelmäßig zu überprüfen**. Dieses Verfahren ist in manchen Bereichen zweifellos sinnvoll, in vielen Fällen aber auch unnötig aufwändig. Für den Bereich des Produktaudits ist dieses Vorgehen nicht praxisgerecht, da die Notwendigkeit einer Überprüfung sich nur ergibt, wenn Änderungen am Produkt erfolgen, oder wenn sich das Umfeld wandelt, z.B. durch Gesetzesänderungen oder Fortentwicklungen der Technik. Vorzuziehen ist, so wie dies in

Schleswig-Holstein praktiziert wird, die Auditierung z.B. auf zwei oder drei Jahre zu befristen und nach der bestimmten Frist eine Reauditierung insofern vorzunehmen, als rechtliche, organisatorische oder technische Veränderungen erfolgt sind. Ergeben sich wesentliche Änderungen zu einem früheren Zeitpunkt, sollte die verantwortliche Stelle verpflichtet werden, dies anzuzeigen, so dass geprüft werden kann, ob eine Nachkontrolle erforderlich ist.

Zu § 2 - Zuständigkeit

Nach Abs. 1 werden die jeweils zuständigen **Datenschutzaufsichtsbehörden** der Länder nach § 38 BDSG bzw. im Bereich der Post und der Telekommunikation der Bundesbeauftragte (BfDI) für Auditierungsfragen für zuständig erklärt. Diesen Behörden werden damit Aufgaben auferlegt, die mit dem derzeit vorhandenen Personal nicht ansatzweise erledigt werden können, wenn die Aufgaben ernsthaft wahrgenommen werden sollen. Sinnvoller wäre es, die präventiv, nicht repressiv auszustaltenden Zertifizierungsaufgaben eigenständigen Stellen zu übertragen, die sich über Gebühren selbst finanzieren.

In Abs. 2 wird die Zuständigkeit für die **Zulassung der Kontrollstellen** und die Entziehung der Zulassung dem BfDI übertragen. Nach Art. 30 GG liegt die Verwaltungszuständigkeit bei den Ländern. Es gibt keinen Grund, diese Aufgaben dem Bund zu übertragen. Die einheitliche Präsentation der Zulassungen kann auch durch eine gemeinsame Stelle der Länder erfolgen.

Zu § 3 - Kontrollen

Gemäß dieser Regelung haben die zugelassenen Kontrollstellen die Auditierung durchzuführen. Nach S. 3 sollen sich Art und Häufigkeit der Kontrollen "nach dem Risiko des Auftretens von Unregelmäßigkeiten und Verstößen in Bezug auf die Erfüllung der Anforderungen dieses Gesetzes und der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen" richten, wobei Kontrollen mindestens einmal jährlich erfolgen sollen. Diese Regelung gibt nicht ansatzweise die Gewähr, dass eine umfassende Überprüfung der Rechtmäßigkeit der Datenverarbeitung stattfindet, da Rhythmus und Prüftiefe der **nicht überprüfbaren Entscheidung der Kontrollstelle** überlassen wird. Im schlechtesten Fall erfolgt die erste Überprüfung 1 Jahr nach der ersten Anzeige (§ 8 Abs. 1; s.u.).

Zu § 4 - Zulassung der Kontrollstellen und Entziehung der Zulassung

Die allgemeinen Anforderungen an Kontrollstellen werden in einer Verordnung nach § 16 Abs. 3 Nr. 2 präzisiert. Dem **BfDI** kommt die Aufgabe zu, die Zulassung zu entziehen. Da jedoch die Kenntniserlangung von Unzulänglichkeiten i.d.R. durch die jeweiligen **Aufsichtsbehörden** erfolgen, wird ein aufwändiges bürokratisches Verfahren etabliert, bei dem letztlich die Feststellung von Rechtsverstößen bei den zertifizierten Stellen zu einem Entzug der Zulassung gegenüber der Kontrollstelle führt bzw. führen kann. Nur die Nichterfüllung der Verpflichtungen des Gesetzes "in schwerwiegender Weise" soll nach Abs. 4 Nr. 2 zur Entziehung der Zulassung führen. Eine derart unbestimmte Regelung gewährt nicht hinreichend die Qualität der Tätigkeit der Kontrollstellen sowie der von ihnen durchzuführenden Kontrollen.

Zu § 5 - Pflichten der Kontrollstellen

Abs. 1 S. 1 verpflichtet Kontrollstellen auf Verlangen zum Abschluss eines Auditvertrages "gegen angemessene Vergütung". Über diesen **Kontrahierungszwang** kann nicht gewährleistet werden, dass von Seiten der Kontrollstellen eine seriöse Auditierung erfolgt. Nach Abs. 1 S. 2 Nr. 2 entfällt der Kontrahierungszwang, wenn "das Durchführen der Kontrollen durch eine andere Kontrollstelle sichergestellt ist". Es wird aber nicht gewährleistet, dass tatsächlich genügend qualifizierte Kontrollstellen bereit stehen. Dies kann zur Folge habe, dass Kontrollstellen zu Kontrollen gezwungen sind, die sie nicht durchführen wollen. Dies hätte keine positiven Auswirkungen auf die Qualität der Kontrolle. Wenn die Kontrollstellen nicht freiwillig die Auditierung durchführen, wird i.d.R. eine qualifizierte Kontrolle nicht stattfinden. Die Entbindung vom Kontrahierungszwang soll beim BfDI oder bei der Aufsichtsbehörde in einem bürokratischen Verfahren erfolgen. Dieses Verfahren hat keinerlei datenschutzrechtlichen Mehrwert.

Der Kontrahierungszwang soll nach Abs. 1 S. 1 nur bestehen, wenn eine „angemessene Vergütung“ erfolgt. Die **Angemessenheit einer Vergütung** lässt sich nur beurteilen, wenn die dafür zu erbringende Leistung hinreichend präzise benannt würde. Dies ist aber nicht möglich. Als Mindestleistung würde eine formale, oberflächliche einjährige Kontrolle ausreichen (§ 3 S. 3). Damit würde aber kein Mehrwert für den Datenschutz erreicht. Je tiefer gehend und qualifizierter eine Prüfung durchgeführt wird, umso höher wäre eine angemessene Vergütung. Angesichts der Komplexität der regelmäßig vorzunehmenden Prüfungen, lässt sich vorab oft eine Beurteilung der Angemessenheit des Kontrollaufwands nicht vornehmen.

Die Kontrollstelle wird in Abs. 2 zu einem **jährlichen Bericht** gegenüber den Aufsichtsbehörden verpflichtet, an den keine inhaltlichen Anforderungen gestellt werden. So ist auch über diesen Bericht nicht gewährleistet, dass qualifizierte Auditierungen durchgeführt werden.

Nach Abs. 3 S. 1 erteilen die Kontrollstellen einander die für die "ordnungsgemäße Durchführung dieses Gesetzes notwendigen **Auskünfte**". Ob diese Übermittlung obligatorisch oder freiwillig sein soll, ergibt sich aus der Regelung nicht. Da die Kontrollstellen zueinander im Wettbewerb stehen, kann nicht davon ausgegangen werden, dass die notwendige Kommunikation tatsächlich stattfindet. Unklar ist auch, welche Auskünfte als erforderlich angesehen werden.

Stellt die Kontrollstelle Datenschutzverstöße fest, so wird sie nach Abs. 3 S. 2, 3 verpflichtet, die zuständige Aufsichtsbehörden und Kontrollstellen zu unterrichten. Um derartige **Unterrichtungen** nicht vornehmen zu müssen, die negative Folgen für die kontrollierte Stelle hätten, wird sich Kontrollstelle veranlasst sehen, so oberflächlich wie möglich zu prüfen. Erfolgt jedoch eine Mitteilung an die Aufsichtsbehörde, so wird das Gegenteil der Entbürokratisierung erreicht, nämlich dass sich mit dem Verstoß sowohl die Kontrollstelle als auch die Aufsichtsbehörde befassen und diese sich insofern koordinieren müssen (vgl. § 6 Abs. 1).

Zu § 6 - Pflichten der zuständigen Behörde

Nach Abs. 1 **überwacht** die Aufsichtsbehörde die **Tätigkeit der Kontrollstelle**. Damit tritt an die Stelle der direkten Kontrolle der Daten verarbeitenden Stelle die Kontrolle der durch die Kontrollstelle durchgeführten Kontrollen. Hierdurch wird - anstelle einer Entlastung der Aufsichtsbehörde - eine zusätzliche Belastung bewirkt. Nach Feststellung eines Datenschutzverstoßes muss nämlich zusätzlich festgestellt werden, wem dieser Verstoß zuzurechnen ist - der unzureichend kontrollierenden Kontrollstelle oder der verantwortlichen Stelle? Im ersteren Fall muss die Aufsichtsbehörde nach Abs. 1 S. 3 die Tatsachen sammeln, die eine Entziehung oder Beschränkung einer Zulassung begründen. Dem schließt sich ein bürokratisches Verfahren der Unterrichtung der für die Entziehung der Zulassung zuständigen Aufsichtsbehörden (v.a. BfDI) an.

Nach Abs. 2 kann die Aufsichtsbehörde die **Entziehung des Datenschutzauditsiegels** anordnen. Gemäß dieser Regelung darf dies aber nur erfolgen, wenn zuvor die Kontrollstelle nach § 5 Abs. 3 S. 2 eine Unterrichtung über einen Datenschutzverstoß vorgenommen hat. Keine Aussage enthält der Entwurf, wenn der Verstoß auf andere Weise der Aufsichtsbehörde bekannt wird. Weitere Voraussetzung ist, dass dieser Entzug "in einem angemessenen Verhältnis" steht. Danach soll das Zertifikat also auch bei Feststellung von Rechtsverstößen beibehalten werden. Dies führt letztlich dazu, dass die Glaubwürdigkeit des Siegels diskreditiert werden kann, zumal es für die Frage, wie die Angemessenheit des Entzugs bewertet werden soll, keinerlei Anhaltspunkte gibt. Bei einem schwerwiegenden Verstoß bzw. einem mit Langzeitwirkung soll eine Auditierung für eine vereinbarte Dauer untersagt werden können. Es ist aber unklar, mit wem die Aufsichtsbehörde die dabei vorgesehene "Vereinbarung" treffen soll.

Zu § 7 - Überwachung

Die Regelung begründet eine umfassende **Auskunftspflicht** sowie Duldungspflichten von den nicht-öffentlichen Stellen und von Kontrollstellen gegenüber den Aufsichtsbehörden. Die Verletzung dieser Vorschrift wäre als Ordnungswidrigkeit zu ahnden (§ 17 Nr. 5). Auch die weiteren Überwachungsbefugnisse der Aufsichtsbehörde sind dem § 38 BDSG nachempfunden.

Nach Abs. 5 sollen die Kontrollbefugnisse der Aufsichtsbehörden **auch für die Kontrollstellen** gelten. Eine

Missachtung dieser Pflicht zur Mitwirkung an der Kontrolle ist jedoch nicht bußgeldbewehrt. Der Regelung ist auch nicht zu entnehmen, welchen Charakter die Auskunfts- und Duldungspflichten gegenüber den Kontrollstellen haben sollen und wie deren Einhaltung durchgesetzt werden kann.

Zu § 8 - Datenschutzauditsiegel, Verzeichnisse

Nach Abs. 1 soll ein Siegel geführt werden können, wenn die Voraussetzungen des § 1 S. 2 erfüllt sind. Voraussetzung ist also nicht, dass dies von der Kontrollstelle positiv festgestellt wird. Es genügt, dass eine Kontrollstelle per Kontrahierungszwang zur Kontrolle verpflichtet wurde. Damit genügt es für die Führung des Siegels, dass man sich zu einer Auditierung verpflichtet, ohne dass tatsächlich ein Audit durchgeführt sein müsste. Nach Abs. 2 besteht keine Nachweispflicht, dass die Anforderungen erfüllt sind. Eine Anzeige gegenüber dem BfDI soll vielmehr genügen. Dieser soll daraufhin die Stelle in ein von ihm zu führendes **Audit-Verzeichnis** aufnehmen, das jedoch nur eine Bezeichnung des Auditierungsgegenstandes enthalten soll, nicht eine Beschreibung und Bewertung.

Außerdem soll der BfDI nach Abs. 2 ein **Verzeichnis der Kontrollstellen** führen.

Zu § 9 - Anforderungen an Kontrollstellen

Die Norm konkretisiert die in § 4 Abs. 1 Nr. 1 genannten Anforderungen an Kontrollstellen. Dabei taucht in Abs. 3 die Differenzierung zwischen rechtlicher und technischer Eignung auf, die in einer Kontrollstelle beide vorhanden sein müssen.

Zu § 10 - Gebühren und Auslagen

Nach Abs. 1 kann der BfDI Gebühren und Auslagen erheben; nach Abs. 2 gilt dies auch für die Aufsichtsbehörden.

Zu § 11 - Datenschutzauditausschuss

Ein Datenschutzauditausschuss soll die **Anforderungen an das Audit** festlegen, soweit die über das bestehende Datenschutzrecht hinausgehen. Gemäß dem Wortlaut darf er keine Gesetzesinterpretation vornehmen, sondern lediglich über das Gesetz hinausgehende Anforderungen formulieren. Um dies aber zu können, bedarf es zunächst einer verbindlichen Feststellung der gesetzlichen Pflichten der verarbeitenden Stellen. Eine derartige bundesweite Feststellung würde aber tendenziell der in Art. 28 Abs. 1 S. 2 EU-DSRL geforderten Unabhängigkeit beeinträchtigen. Als Beispiele für die Übererfüllung gesetzlicher Regeln werden in Abs. 1 S. 2 genannt: Transparenz, Datensparsamkeit und Stärkung der Stellen des betrieblichen Datenschutzbeauftragten. Dabei wird verkannt, dass die zentralen Fragen einer Auditierung in Bereich der Auslegung des materiellen Rechts und der technisch-organisatorischen Maßnahmen liegen. Hierbei sind wegen der vielen unterschiedlichen möglichen Anwendungsfälle und wegen der sich dauernd weiter entwickelnden Technik die Anforderungen nicht einheitlich festzulegen. Es lassen sich allenfalls für bestimmte Anwendungen (z.B. Videoüberwachung, Online-Shops, Archivierungssysteme, Auswertungsverfahren medizinischer Daten) Schutzprofile entwickeln, denen aber wegen der jeweils weiterhin möglichen Fallgestaltungen nur beispielhafter Empfehlungscharakter zukommen kann, nicht aber förmliche Verbindlichkeit. Es ist nicht ansatzweise praktisch vorstellbar, in welcher Form der Datenschutzausschuss seiner Aufgabe zur Festlegung von Richtlinien nachkommen soll.

Zu § 12 - Mitglieder des Datenschutzauditausschusses

Die Regelung bestimmt die **Zusammensetzung**, also welche Vertreter von Interessengruppen bzw. Institutionen an dem Ausschuss beteiligt werden soll: 2 Verwaltung Bund, 2 Bundesamt für Sicherheit in der Informationstechnik, 2 BfDI, 2 Verwaltung Länder, 4 Landes-Aufsichtsbehörden, 6 Wirtschaft. Nicht erklärlich ist, weshalb völlig Fachfremde an dem Ausschuss beteiligt werden (Verwaltung Bund, Länder), nicht aber Vertreter der Betroffenen (Verbraucherverbände, Arbeitnehmervertreter). Die Darstellung in der Begründung, dass Vertreter der Verwaltung des Bundes und der Länder "in verschiedener Weise für fachspezifische Vorschriften des Datenschutzes zuständig" seien, ist nicht nachvollziehbar. Nach Abs. 1 S. 2 soll die

Tätigkeit der Ausschussmitglieder nicht nur weisungsfrei, sondern auch ehrenamtlich, d.h. grundsätzlich unentgeltlich sein. Angesichts der geforderten hohen Qualifikation und des mit der Tätigkeit verbundenen Aufwands - wenn diese wirkungsvoll sein soll - ist es befremdlich, dass hierfür keine Bezahlung erfolgen soll. Dies führt wohl dazu, dass die entsendenden Einrichtungen vorrangig Interessenvertreter benennen, die dann aber nicht in der intendierten Unabhängigkeit agieren können. An der Unabhängigkeit der Ausschusstätigkeit entstehen auch insofern Zweifel, als nach Abs. 3 - wohl im Einvernehmen mit dem BfDI, den obersten Landesbehörden, den Aufsichtsbehörden und den Wirtschaftsverbänden - die Berufung durch das Bundesministerium des Innern erfolgen soll. Das aufwändige Bestellungsverfahren ist ein bürokratischer Vorgang, der keinerlei positive Effekte für den Datenschutz entfaltet.

Zu § 13 - Geschäftsordnung, Vorsitz und Beschlussfassung des Datenschutzauditausschusses

Die Geschäftsordnung des Ausschusses bedarf nach Abs. 1 der Genehmigung durch das Bundesministerium des Innern (BMI). Der Ausschuss beschließt nach Abs. 3 Nr. 1 über die "Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit" nach § 11 Abs. 1 S. 2 mit der Mehrheit von zwei Dritteln. Dies hätte zur Folge, dass die Richtlinien geprägt wären von **Kompromissen**.

Zu § 15 - Rechtsaufsicht

Nach Abs. 1 und 2 soll der Ausschuss der Aufsicht des BMI unterliegen, das gegenüber dem Auschuss weitgehende direktive Kompetenzen erhält. Nach Abs. 3 S. 1 müssen Richtlinienbeschlüsse durch die Aufsichtsbehörde, also das BMI, genehmigt werden. Nach Abs. 4 hat das BMI sogar das Recht, den Datenschutzauditausschuss aufzulösen. Angesichts eines derart **rigiden und bürokratischen Verfahrens** bestehen Zweifel, ob der Ausschuss die ihm auferlegten Aufgaben wirksam und unabhängig erfüllen kann. Die technischen und rechtlichen Herausforderungen verlangen Flexibilität und schnelle Reaktionsfähigkeit. Es könnte sich der Zustand einstellen, dass die Tätigkeit des Ausschusses eher innovationshindernd als –fördernd ist.

Zu § 16 - Verordnungsermächtigungen

Die Abs. 1 und 2 sehen vor, dass zugelassene Kontrollstellen von den Ländern bzw. vom BMI mit den Aufgaben der staatlichen Aufsicht beliehen werden können. Die Notwendigkeit einer solchen **Beleihung** ist nicht erkennbar. Die Übertragung der Kontrolle von Privaten, die Aufgaben der staatlichen Aufsicht wahrnehmen sollen, auf weitere Private, die zugleich mit den Kontrollierten in Konkurrenz stehen, wäre ein Sichentziehen aus der Verantwortung durch den Staat. Die Beleihung soll v.a. durch das BMI erfolgen, was wohl mit Art. 28 Abs. 1 S. 2 EU-DSRL nicht vereinbar ist, da eine Aufgabe des europarechtlich unabhängigen BfDI (bzw. der Landesbehörde) auf ein privates Unternehmen übertragen würde, das (wohl?) der Rechtsaufsicht des BMI unterläge.

Nach Abs. 3 erhält das BMI die Ermächtigung zum Erlass einer Rechtsvorordnung, in der alle Einzelheiten "über die Voraussetzungen und das Verfahren der Zulassung ... sowie ... der Entziehung der Zulassung" von Kontrollstellen sowie die "Mindestkontrollanforderungen und im Rahmen des **Kontrollverfahrens** vorgesehene Vorkehrungen festzulegen" sind. Es bestehen Zweifel, dass mit einer derart rigiden Regulierung durch das BMI, das selbst über keinerlei praktische Kontrollerfahrung verfügt, hinreichende Voraussetzungen für die freiwillige Nutzung des Auditinstruments geschaffen werden können.

Zu § 17 - Bußgeldvorschrift

Für die Verletzung von formellen Pflichten soll eine Geldbuße bis zu 300.000 Euro verhängt werden können. Diese Bußgeldhöhe steht im Widerspruch zu dem parallelen geplanten § 43 Abs. 3 BDSG, wonach die maximale **Bußgeldhöhe** bei formellen Verstößen gegen das BDSG mit 50.000 Euro vorgesehen ist. Dies hätte zur Folge, dass bei Teilnahme an dem freiwilligen Audit das Bußgeldrisiko versechsfacht würde, was der Bereitschaft zur Teilnahme für Unternehmen nicht förderlich wäre.

Zu § 18 - Strafvorschrift

Der **Abschreckungseffekt** von einer Auditierung würde durch die Strafandrohung bei absichtsvoller unbefugter Verwendung des Datenschutzauditsiegels noch weiter erhöht. Eine strafrechtliche Sanktionierung bei formellen Verstößen war und ist im BDSG bisher nicht vorgesehen.

Zu § 19 - Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Danach ist eine auditierte Stelle, entgegen der Regelung des geplanten § 44a BDSG, bei bestimmten unzulässigen Übermittlungen und bei Datenlecks nicht zur Benachrichtigung gegenüber der Aufsichtsbehörde, sondern gegenüber der Kontrollstelle verpflichtet. Welche Konsequenzen diese ziehen soll, ergibt sich aus der Regelung nicht. Aus § 5 Abs. 3 S. 2 ergibt sich aber wohl eine weitere Informationspflicht der Kontrollstelle gegenüber der Aufsichtsbehörde, wie dies ohnehin geboten wäre. Es ist daher nicht nachvollziehbar, weshalb die Begründung davon spricht, dass durch diese Regelung eine **Begrenzung der Benachrichtigung** auf die Kontrollstelle erfolgen würde.