

Stellungnahme des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

**Zum Entwurf eines Gesetzes zur Änderung des
Bundesdatenschutzgesetzes und zur Regelung des Datenschutzaudits vom
22.10.2008**

Berlin, 30.10.2008

A. Allgemein zum Gesetzentwurf

Mit dem Gesetzentwurf vom 22.10.2008 zur Änderung des Bundesdatenschutzgesetzes reagiert die Bundesregierung auf Datenschutzskandale der jüngsten Zeit. Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. begrüßt grundsätzlich, dass die in der Praxis festgestellten Defizite durch zügige Änderungen der gesetzlichen Rahmenbedingungen behoben werden sollen.

Diese Überarbeitung bietet die Chance, das Bundesdatenschutzgesetz in wichtigen Punkten klarer und konkreter zu fassen und gleichzeitig Verbesserungen zur Stellung des DSB, zur Einwilligung in die Datenverarbeitung und zu den Informationspflichten zu erzielen. In der vorliegenden Form würden allerdings viele der vorgeschlagenen Änderungen das Bundesdatenschutzgesetz unnötig verkomplizieren und so eine weitere Bürokratisierung des Datenschutzes bewirken.

Der Gesetzentwurf ist im Ergebnis insgesamt unbefriedigend, denn er löst lediglich punktuell einige Fragenstellungen bei der Datenverwendung zur Werbung, Markt- und Meinungsforschung. Nach wie vor mangelt es an einer grundlegenden Änderung des Datenschutzgesetzes. Es bleibt zu befürchten, dass auch in Zukunft einzelne Vorschriften des BDSG erst nach Datenschutzskandalen geändert werden, ohne endlich die grundlegenden Probleme zu lösen.

Der Gesetzentwurf beantwortet in keiner Weise die dringenden Fragen zur Zulässigkeit von Datenverwendungen wie z.B. im Arbeitsverhältnis, bei der Verwendung von Daten in öffentlichen Netzen oder beim Einsatz von Überwachungstechniken. Zahlreiche unbestimmte Regelungen wurden nicht konkretisiert.

Die Idee, die Rechtstellung des Datenschutzbeauftragten zu stärken, um präventiv den Datenmissbrauchsmöglichkeiten etwas entgegenzusetzen, ist misslungen. Eine Regelung zur Kostentragung von Fortbildungen beseitigt nicht den Missstand, dass es überhaupt keinen Standard für die Qualifikation von Datenschutzbeauftragten gibt und beseitigt auch nicht die vorhandenen Schwierigkeiten in der beruflichen Praxis des Datenschutzbeauftragten. Weder werden ihm notwendige Rechtspositionen wie zum Beispiel der unerlässliche Kündigungsschutz eingeräumt, noch finden seine Prüfungsaufgaben nachhaltig im Gesetz Einzug.

Defizite im Gesetzesvollzug wie fehlende Bußgeldvorschriften werden nicht beseitigt. Auch neuere Instrumente wie eine ausgeprägte Transparenz der Datenverarbeitung oder zu veröffentlichende Prüfungsberichte finden keinen Eingang in den Gesetzentwurf.

Der Entwurf eines Datenschutzauditgesetzes ist grundsätzlich positiv und füllt endlich eine gesetzliche Lücke, dennoch besteht auch hier Korrekturbedarf bei zahlreichen Punkten.

B. Artikel 1, Änderung des Bundesdatenschutzgesetzes

I. Zu Punkt 2: Änderung § 4f Abs. 3 - Fortbildungskostenübernahme für den DSB

Die Zielrichtung, die Position des Datenschutzbeauftragten zu stärken, ist begrüßenswert und richtig. Das gewählte Mittel, der verantwortlichen Stelle die Kosten für die Fortbildung des Datenschutzbeauftragten ausdrücklich aufzubürden, ist jedoch weder ausreichend noch zielführend; die Beschränkung auf diese Kostenübernahme ist hingegen gefährlich und kontraproduktiv. Es fehlt eine Regelung zur effektiven Verbesserung der Rechtsposition des Datenschutzbeauftragten.

Durch die vorgeschlagene Regelung werden Unternehmen zur Kostenübernahme von Fortbildungen verpflichtet, ohne dass die Anforderungen an die Fortbildung oder an die Ausbildungsstellen definiert sind. Es gibt weder Qualitätsanforderungen noch Mindeststandards für die Aus- und Fortbildung von Datenschutzbeauftragten. Welche Fortbildungsinhalte werden in einer solchen Situation gefördert? Wenn jemand - wie vorgeschlagen - zur allgemeinen Kostenübernahme verpflichtet werden soll, bleibt ohne Qualitätskriterien der Preis das einzige Steuerungskriterium. Der Gesetzgeber fördert damit den Wettbewerb der billigsten Aus- und Weiterbilder im Datenschutz; der Bezug zu qualitativen Anforderungen fehlt gänzlich und wird so unterdrückt. Durch eine solche qualitätsunabhängige Pflicht ist eine Wettbewerbsverzerrung zu Ungunsten der wenigen seriösen Weiterbildungsstellen zu erwarten; es werden insbesondere die x-beliebigen „Billig-Schulungsanbieter“ unterstützt, die weder fähig noch fachlich in der Lage sind, Datenschutzwissen zu vermitteln.

Darüber hinaus löst diese Verpflichtung nicht die weiteren Schwierigkeiten des Datenschutzbeauftragten. Auch wenn sich der Datenschutzbeauftragte fortbildet, steht er vor dem Problem, dass er nicht oder viel zu spät in Planungen einbezogen wird, von Überprüfungen ausgeschlossen bleibt, nicht rechtzeitig informiert wird, unter Druck gesetzt werden kann. Der schwache Kündigungsschutz verhindert nach wie vor eine objektive, unabhängige Prüfungsmöglichkeit durch den angestellten Datenschutzbeauftragten. Beantwortet wird auch nicht die Frage, wie der Datenschutzbeauftragte seine Aufgaben wahrnehmen soll.

Das Ziel, die Position des Datenschutzbeauftragten zu stärken, lässt sich effektiv nur durch andere Vorgaben erreichen. Dazu gehören u.a. folgende Maßnahmen, die im Gesetz verankert werden müssen:

- Ein erweiterter Kündigungsschutz für Datenschutzbeauftragte, wie ursprünglich in diesem Entwurf geplant,
- Informations- und Beteiligungspflichten für Datenschutzbeauftragte bei datenschutzrelevanten Verfahren,
- ein klarer Prüfungsauftrag für die Datenschutzbeauftragten,
- die Normierung der Aufgabe des Datenschutzbeauftragten, die wahrheitsgemäßen Offenlegung und die Einhaltung der offengelegten Verarbeitungsgrundsätze zu kontrollieren,
- die Veröffentlichung von Datenschutz-Prüfungsergebnissen und die Einführung eines verpflichtenden Datenschutzjahresberichts.

II. Zu Nr. 5: Änderung § 28 Abs.2/3 – Erlaubnis zur Datenverwendung für andere Zwecke

Die Zusammenfassung der Erlaubnis, Daten für andere Zwecke zu verwenden, ist zu begrüßen. Die vorgesehene Zusammenführung von Abs.2 und 3 vereinfacht das Verständnis, was das Gesetz erlaubt.

Positiv hervorzuheben ist, dass erstmalig mehrere Fallgruppen im Gesetz formuliert werden, um darzustellen, wann das berechnigte Interesse eines Betroffenen an einem Verarbeitungsvorgang auszuschließen bzw. anzunehmen ist. Eine solche Auflistung unterstützt die praktische Arbeit, die unbestimmten Rechtsbegriffe und Auslegungsfähigkeiten von „berechtigtem Interesse“ und „überwiegen“ zielsicherer anzuwenden.

Dabei ist für die Praxis sehr hilfreich, dass eine Kernbeschränkung in der Datenverwendung zur Markt- und Meinungsforschung gesetzt wird: § 28 Abs.3 Nr.1 beschränkt die Verwendung der Daten zur Verarbeitung zu eigenen Zwecken und beschränkt auf Daten, die direkt erhoben wurden. Dies erscheint interessengerecht und beschränkt die in der Praxis schwer zu überwachende „Wanderung“ von Adresdaten.

III. Weiter Zu Nr.5: § 28 Abs.3a und 3b - Anforderungen an die Einwilligung

Die Konkretisierung von Anforderungen an eine Einwilligung ist zu begrüßen. Die genannten Punkte erläutern die bisher unklaren Begriffe in § 4a „andere angemessene Form“ und „besonders hervorzuheben“.

Es ist allerdings nicht nachvollziehbar, warum diese Konkretisierung einer Einwilligung nur bei Einwilligungen für die Fälle des § 28 Abs.3, also der Markt- und Meinungsforschung, gelten sollen. Die hier genannten Anforderungen an eine Einwilligung sind nicht ungewöhnlich und bereits heute gute Praxis für verschiedene Einwilligungssituationen. Die Schriftform ist in den meisten Fällen das einzige Mittel zur Dokumentation der Einwilligung und nichts Besonderes. Die Positionierung dieser Anforderungen im § 28 lässt eher befürchten, dass andere Einwilligungen diese Anforderungen nicht erfüllen müssen oder dürfen, je nach Standpunkt. Die praktischen Schwierigkeiten des § 4a bleiben weiterhin bestehen, und noch mehr: Nun muss der Datenschutzbeauftragte diese Einwilligung nach § 4a abgrenzen von der Einwilligung nach § 28 Abs.3a. Eine solche Splittung trägt zur Verkomplizierung und Bürokratisierung des Datenschutzes bei.

Stattdessen sollten die Anforderungen an eine Einwilligung in den „allgemein Teil“ des BDSG aufgenommen werden, in § 4a. Die unklaren Anforderungen in § 4a, die in der Praxis viele Fragen an die richtige Einwilligung aufwerfen, sollten durch eine Konkretisierung, wie in § 28 Abs.3a vorgeschlagen, ersetzt werden. Außerdem sollte ein Gleichklang mit Einwilligungsanforderungen in anderen Vorschriften, z.B. im TMG, erzielt werden. Der Gesetzgeber sollte sich auf eine allgemein verständliche Form festlegen, wie eine Person ihren Willen zu einer Datenverwendung äußern sollte, so dass die Person und der Datenverwender, also alle Seiten, Klarheit darüber haben, was die Person möchte und was nicht. Die Formulierungen des § 28 Abs.3a sind hierzu ein guter Ansatz, müssen aber allgemein für alle Verarbeitungen gelten.

IV. Zu Nr.7: § 33 – Informationspflicht an den Betroffenen

Die vorgeschlagenen Änderungen zum § 33 sind unzureichend und geben keine Antwort auf die praktischen Probleme mit dieser Vorschrift.

Die Unterrichtungspflicht gegenüber den Betroffenen nach § 33 ist generell unpraktikabel und zu kompliziert. Die Trennung in eine Informationspflicht bei erstmaliger Speicherung und in eine Informationspflicht bei erstmaliger Übermittlung in den Fällen der Speicherung zur geschäftsmäßigen Übermittlung macht seit je her wenig praktischen Sinn. Auch die Information über die Empfänger nur für den Fall, dass der Betroffene nicht mit der Übermittlung rechnen konnte, verkompliziert diese Informationspflicht. In der Praxis stehen Unternehmen oft vor der Frage, ob sie eine

Informationspflicht haben oder nicht. Das Ziel, den Betroffenen die Verarbeitungsvorgänge transparent zu machen, wird in der Praxis nicht erreicht.

§ 33 sollte daher umfassend geändert werden. Es ist eine verständliche, für alle geltende Informationspflicht zu formulieren. So sollte festgelegt werden, dass Betroffene bei der Speicherung von Daten zu informieren sind über:

- die einzelnen Zwecke der Datenverarbeitung und -nutzung,
- die an der Verarbeitung beteiligten Stellen,
- über die Art und Menge der verwendeten Daten,
- die Nutzungsarten, einschließlich detaillierter Informationen über den Weg, den die Daten im Verantwortungsbereich oder auf unmittelbaren Anlass der verarbeitenden Stelle nehmen,
- die Speicherdauer und
- die tatsächliche Herkunft der Daten.

Die Informationspflicht ist für alle speichernden Stellen gleich und unabhängig vom Verwendungszweck zu gestalten.

V. Zu Nr. 8: § 43 – Erweiterung des Bußgeldkataloges

Die vorgeschlagenen Änderungen im Bußgeldkatalog beheben nicht die bestehenden Defizite im Gesetzesvollzug.

In der Praxis hat sich gezeigt, dass verschiedene Pflichten des BDSG nicht umgesetzt werden, weil u.a. eine Sanktionierung bei Nichterfüllung fehlt. Das Nichteinhalten wichtiger Vorgaben wie die Ergreifung von technisch-organisatorischen Schutzmaßnahmen oder das Führen eines Verfahrensverzeichnisses wird überhaupt nicht sanktioniert, andere Tatbestände sind so allgemein gehalten, dass Verstöße gegen essentielle Datenschutzanforderungen nur in besonders klaren Fällen erfasst sind. Dieses Problem wird erneut nicht behoben.

Die vorgeschlagene Verdoppelung des maximalen Bußgeldbetrages reicht zudem nicht aus, zum gesetzestreuem Verhalten zu motivieren. In der Praxis stellen verantwortliche Stellen häufig vor einer Entscheidung die wirtschaftliche Frage: Was kostet die Erfüllung der Pflicht und was kostet die Nichterfüllung der Pflicht? Sie entscheiden sich für die kostengünstigere Variante. Dieses Problem eines „preiswerten“ Gesetzesverstößes muss behoben werden.

Zur Lösung sollten folgende Änderungen umgesetzt werden:

Die Tatbestände der sanktionierten Datenschutzverletzungen sind zu erweitern. Dazu gehören die Sanktionierung von:

- mangelhafter Transparenz der Datenverarbeitung,
- fehlerhafter Offenlegung von Verarbeitungsvorgängen,
- mangelhafter Umsetzung von Schutzmaßnahmen,
- fehlenden Verfahrensübersichten sowie
- Bestellungen nicht qualifizierter „Alibi-Datenschutzbeauftragter“.

Die Bußgeldhöhe ist mindestens zu verdreifachen. Die Ergänzung durch den neuen Absatz 3, wonach beim Übersteigen des wirtschaftlichen Wertes die Bußgeldgrenze überschritten werden kann, ist sinnvoll. Dies reicht allerdings nicht aus, das Problem zu lösen. Diese Vorschrift setzt nämlich in der Praxis voraus, dass sich der wirtschaftliche Wert tatsächlich für die bußgeldverhängende Stelle bemessen lässt.

VI. Zu Nr.9: § 44a – Informationspflicht

Die Informationspflicht über Datenschutzverletzungen ist grundsätzlich positiv. Diese Regelung ist neu und knüpft an positive Erfahrungen aus den USA an.

Die vorgeschlagene Informationspflicht ist allerdings wenig praktikabel. Der Bereich der Vorfälle, über die informiert werden muss, ist erheblich eingeschränkt. Erfahrungsgemäß sind die Datenverarbeitungen, die hier angesprochen sind (Verarbeitung besonderer Art der Daten, schweigepflichtige Daten) oft wesentlich besser gestaltet als die vielen Verarbeitungsvorgänge mit anderen personenbezogenen Daten. Die Datenverletzungen bei den vielen Verarbeitungen mit laienhaften Schutzmaßnahmen werden gar nicht erfasst.

Es ist auch kein sachlicher Grund erkennbar, diverse Verarbeitungen und verarbeitende Stellen von der Informationspflicht auszunehmen.

Darüber hinaus ist die Regelung völlig unübersichtlich und anwenderunfreundlich. Mehrere Anforderungen werden in einem Fließtext miteinander vermengt. Diese Regelung muss dringend dahingehend überarbeitet werden.

Die gesetzliche Regelung sollte für Nichtjuristen praktikabel gefasst werden. Die Informationspflicht in § 44a sollte mehrere Fragen beantworten, und zwar getrennt in mehreren Absätzen:

- Wer hat eine Informationspflicht
- Wann muss informiert werden (Auflistung aller Voraussetzungen)
- Wer muss informiert werden
- Wie muss informiert werden

Ungeregt ist bisher, wie die Nichteinhaltung der Informationspflicht sanktioniert wird.

C. Artikel 2: Datenschutzauditgesetz

I. Zu § 1: Anwendungsbereich

Die Beschränkung des Audits auf reine nicht öffentliche Stellen ist nicht vorteilhaft. Auch öffentliche Stellen sollten die Möglichkeit haben, ein Datenschutzauditsiegel zu verwenden - ebenfalls freiwillig: Das DSAG sollte an dieser Stelle Vorbildfunktion für die notwendige Novellierungen der Landesdatenschutzgesetze haben. Die Landesdatenschutzgesetze könnten sich mit Kontrollstellen etc. am DSAG orientieren. So könnte das jetzt vorherrschende Chaos bei den 17 Varianten der technischen und organisatorischen Maßnahmen vermieden werden, wenn sich beispielsweise jedes Bundesland auf die Richtlinien gemäß §11 beziehen könnte und diese nicht selbst definiert. Erst dann wäre ein einheitliches Datenschutzauditsiegel in Deutschland denkbar. Die unterschiedlichsten Siegel, Zertifikate, ISO-Zertifizierungen, Qualitätsmanagement-Urkunden, etc. sind für den Bürger nicht durchschaubar. Zwar haben, wie die Begründung zum Gesetzentwurf beschreibt, die Bürger mit wenig öffentliche Stellen des Bundes zu tun, und ein Wahlrecht besteht auch nicht bezüglich Behörden wie Stadtverwaltungen oder Landratsamt. Allerdings finden landesrechtliche Vorschriften auch auf Einrichtungen wie Krankenhäuser und Kindergärten Anwendung, bei denen durchaus ein Wahlrecht besteht. Schließlich könnten öffentliche Stellen durch eine Auditierung eine Vorbildfunktion übernehmen und die Datenschutzkultur fördern.

II. Noch zu § 1: Inhaltlicher Anwendungsbereich

Die Beschränkung auf eine einzelne Datenverarbeitung ist vom Prinzip her sinnvoll: Für einen ganzen Betrieb kann man die Einhaltung der Datenschutzvorschriften nicht bestätigen. Allerdings lässt das Gesetz einen entscheidenden Faktor vermissen: Eine getrennte Betrachtung von zu zertifizierenden Produkten wie Software einerseits, und Unternehmensprozesse andererseits. Die Einhaltung von Datenschutzvorschriften ist für ein Produkt schon systembedingt anders zu sehen und einzuordnen als für ein Unternehmensprozess. Diese Anforderung erfüllt der Gesetzentwurf nicht. Der Gesetzentwurf zeigt vielmehr, dass eine Zertifizierung von Produkten nicht durch das Gesetz abgedeckt ist, denn die in Punkt genannte Anforderung „Einhaltung der Vorschriften des Bundesdatenschutzgesetzes über die organisatorische Stellung des Beauftragten für den Datenschutz“ macht für ein Produkt keinen Sinn.

Positiv zu vermerken ist, dass der Datenschutzbeauftragte selbst nicht im Rahmen eines solchen Audits geprüft wird. Dies würde seine unabhängige Stellung beeinflussen. Warum allerdings nur die ordnungsgemäße Einbindung eines Datenschutzbeauftragten geprüft werden soll, ist nicht klar. Sinnvoll und aussagekräftiger wäre eine Prüfung des gesamten Datenschutzmanagements der jeweiligen Stelle.

III. Zu § 3: Kontrollstellen, Fristen

Positiv hervorzuheben ist, dass ein jährlicher Zeitraum für die Kontrolle festgelegt wird. Dies stellt sicher, dass die Anforderungen in einer sich schnell ändernden technischen Welt erfüllt bleiben. Positiv ist auch, dass der Datenschutzbeauftragte einbezogen werden soll.

Es stellt sich allerdings die Frage, ob ein Unternehmen, das einen Prozess auditiert, nicht zwingend einen Datenschutzbeauftragten bestellt haben muss. In der Gesetzesbegründung wird dies verneint. Das erscheint nicht logisch. Das Gesetz baut darauf, dass außerhalb der Auditierungszeitpunkte der Datenschutzbeauftragte für die Einhaltung der Datenschutzvorschriften sorgt, und er aus diesem

Grunde auch in die Auditierung einbezogen wird. Wenn aber kein Datenschutzbeauftragter existiert, weil nach dem BDSG-Regeln kein Beauftragter bestellt werden muss, wird das Ziel des Gesetzes nicht erreicht. Auf die Bestimmungsregeln des BDSG zu verweisen, setzt den Anspruch des DSAG außer Kraft.

IV. Zu § 3 und § 4: Kontrollstellen (auch § 9)

Die Einrichtung privater Kontrollstellen ist grundsätzlich zu begrüßen. Es gibt keine Gesetzmäßigkeit, dass trotz komplexer Vorgänge und einer permanenten Weiterentwicklung der Anforderungen dies durch rein staatliche Stellen besser umgesetzt werden könnte. Der Einsatz von privaten Kontrollstellen setzt aber voraus, dass eine effektive und nachhaltige Qualitätssicherung der Kontrollstellen stattfindet.

Dazu gehört die bereits vorgesehene Zulassungspflicht. Anders als bei einer Registrierung oder Anmeldung wird eine Prüfung der Voraussetzungen beabsichtigt. Positiv hervorzuheben ist dabei, dass die besondere Eignung nicht nur für die Leitungsperson der Kontrollstelle, sondern auch für die tatsächlich kontrollierenden Personen vorliegen muss. Dies sichert eine Durchdringung der Qualität.

Unklar ist jedoch, wie die Qualitätseigenschaften nachgewiesen werden müssen und welche Kriterien die Eigenschaften ausmachen. Der Verweis auf § 9 hilft hier nicht weiter. So sagt z.B. § 9 Abs.1, dass die Zuverlässigkeit bei den Personen gegeben ist, wenn sie aufgrund der persönlichen Eigenschaften, des Verhaltens und der Fähigkeiten geeignet ist. Wie man das allerdings nachweist, bleibt unklar. Einige persönliche Eigenschaften sind die § 9 aufgelistet, bei deren Vorliegen Zuverlässigkeit oder Unabhängigkeit nicht gegeben sind. Ob in den Fällen, in denen kein Ausschlusskriterium vorliegt, Unabhängigkeit und Zuverlässigkeit immer vorliegen oder ob dies positiv festgestellt werden muss, erschließt sich nicht.

Es fehlt zudem an einer Sicherstellung der einmal festgestellten Qualität. Zwar können Beschränkungen und Auflagen festgesetzt werden, diese Einschränkung ist jedoch nur eine allgemeine Kannvorschrift und keine Voraussetzungen für alle Kontrollstellen. Notwendig für die Aufrechterhaltung von Qualität wären z.B. eine generelle Befristung, eine Fortbildungspflicht oder Ereignisse, in denen die Zulassung erlischt.

Hilfreich für die Qualitätssicherung ist auch eine Beschreibung eines Verfahrens, wie verantwortliche Stellen, die sich zertifizieren lassen möchten, die rechtmäßige Zulassung einer Kontrollstelle überprüfen können. Hier sollten Anreize geschaffen werden, dass sich eine Kontrollstelle auch einer potentiellen Gegenkontrolle stellen muss, um Qualitätsverlust oder Missbrauch zu verhindern.

Aufrechterhalten werden sollte die im Entwurf getroffene Regelung, dass die persönlichen Anforderungen von jeder einzelnen beteiligten Person, also Personen der Leitung als auch der Ausführung, verlangt werden.

V. Zu § 5: Kontrollverfahren

Unklar ist, wie eine Kontrollstelle die Erfüllung der Anforderungen überprüft. Zwar beschreibt § 7 allgemeine Dinge zur Überwachung; welche Prüfungspflichten bestehen, wird nicht deutlich. Die Kontrollstelle hat lediglich die Pflicht, einmal jährlich geprüfte Stellen zu melden. Warum und Wie geprüft wurde, bleibt unklar. Dieses Verfahren stellt nicht sicher, dass eine Kontrollstelle ordnungsgemäß prüft.

VI. Zu § 6: Siegelverlust

Der Behörde wird ein Recht eingeräumt, die Verwendung des Datenschutzsiegels bei Unregelmäßigkeiten zu untersagen. Diese Vorschrift ist kritisch zu sehen, denn sie hebt das Ziel eines Audits aus: Trotz festgestellter Mängel kann ein Siegel weiter verwendet werden. Wenn aber ein Siegel nur dann erworben werden kann, wenn bestimmte Anforderungen erfüllt sind, muss die Berechtigung zur Siegelführung sofort und zwangsläufig wieder entfallen, wenn die anspruchsbegründenden Anforderungen nicht mehr erfüllt sind. Gestattet man Abweichungen, wird das Siegel abgewertet. Der Sinn eines Datenschutzaudits wird durch das Gesetz selbst gefährdet.

VII. Zu § 8: Anzeigepflicht für Datenschutzsiegel

Die Führung eines Datenschutzsiegels muss vorab angezeigt werden. Allerdings reicht dieser Schritt nicht aus, um die Vergabe eines Siegels transparent zu gestalten und Missbrauch zu verhindern. Allein die Existenz eines Siegels erklärt nicht, welche Kriterien zur Siegelführung berechtigen. Da Datenschutzkonzept und technische Einrichtungen zertifiziert werden können, besagt ein Siegel noch nicht, welche Dinge mit dem Siegel bestätigt werden.

VIII. Zu § 10 und 11: Ausschuss

Sowohl die Zusammensetzung, als auch die Aufgaben des Ausschusses werfen Fragen auf.

Positiv ist, dass jederzeit Maßstäbe aufgestellt und angepasst werden können, so dass aktuelle Anforderungen und Erkenntnisse berücksichtigt werden können. Allerdings ist nicht klar, wie die Richtlinien Verbesserungen in den genannten Datenschutzbereichen vorschreiben können. Hier ist nicht erkennbar, anhand welcher Kriterien der Ausschuss tatsächlich Verbesserungen statt Auslegungen der geltenden Gesetze formuliert. Datenschutzerfordernisse sind häufig durch unbestimmte Rechtsbegriffe festgelegt. Es ist zu befürchten, dass diese Richtlinien praktisch nur Hilfen bei der Interpretation dieser Vorschriften werden.

Die Zusammensetzung des Ausschusses erklärt sich nicht. Vertreter von Bundes- und Landesbehörden sollen dem Ausschuss angehören, ohne dass deren fachliche Eignung geklärt ist. Welchen praktischen Beitrag diese für fachliche Datenschutzrichtlinien liefern können, ist kritisch zu hinterfragen. Fachlich geeignet ist hingegen der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.. Er vertritt die betrieblichen und behördlichen Datenschutzbeauftragten und damit die Berufsgruppe, die dem Datenschutzauditor am nächsten kommt und fachlich besser geeignet ist. Der BvD fehlt jedoch als Mitglied des Ausschusses.