

Stellungnahme

Entwurf eines Bundesdatenschutzauditgesetzes

22. Oktober 2007

Seite 1

Der BITKOM vertritt mehr als 1.000 Unternehmen, davon 850 Direktmitglieder mit 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT- und Telekommunikationsdiensten sowie Content. BITKOM setzt sich insbesondere für eine Verbesserung der ordnungsrechtlichen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.

Untrennbar verbunden mit dem Engagement des BITKOM für die Entwicklung der Informationsgesellschaft ist der Einsatz für einen modernen und technikadäquaten Datenschutz. Vor dem Hintergrund der anhaltenden Auseinandersetzung um Datenschutz-Gütesiegel und Datenschutzaudits als Gewähr für Datenschutz ist es BITKOM wichtig, aus Sicht der Betroffenen auf verschiedene Gesichtspunkte hinzuweisen, die bislang nicht die erforderliche Beachtung gefunden haben.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Dr. Kai Kuhlmann
Bereichsleiter Recht
Tel. +49. 30. 27576-131
Fax +49. 30. 27576-139
k.kuhlmann@bitkom.org

Präsident

Prof. Dr. Dr. h. c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer

Dr. Bernhard Rohleder

1. Allgemeine Erwägungen: Bedarf und Nutzen

Ausgangspunkt des Gesetzgebungsvorhabens zu einem Bundesdatenschutzaudit-Gesetz ist § 9 a BDSG, der die gesetzliche Regelung eines Audits ermöglicht:

„Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“

Ungeachtet des Umstands, dass die Möglichkeit eines Datenschutzaudits und seine gesetzliche Regelung im BDSG angelegt sind, ist nach Auffassung des BITKOM der Sinn zweifelhaft – eine Eignung als Differenzierungskriterium im Wettbewerb sehen unsere Mitgliedsunternehmen nur punktuell. Unsere wesentlichen Bedenken in Bezug auf ein Datenschutzaudit-Gesetz und dessen beabsichtigten Zusatznutzen haben wir in den letzten Jahren wiederholt dargelegt. Sie lassen sich wie folgt zusammenfassen:

Das Anliegen des Gesetzgebers bei der Aufnahme des § 9 a BDSG war es, die Intentionen und Vorgaben des BDSG dadurch zu verstärken, dass datenverarbeitende Stellen und Anbieter ihre Verfahren bzw. Produkte freiwillig in einem externen Qualitätsprüfungsprogramm begutachten lassen. Bei erfolgreicher Auditierung soll ein Zusatznutzen erreicht werden, insbesondere ein positives Image des Unternehmens, Stärkung des Vertrauens und Marktvorteile. Zugleich soll (so die Begründung des Entwurfs) dem Verbraucher die Möglichkeit einer Marktorientierung bezüglich datenschutzgerechter Produkte bzw. Dienstleistungen gegeben werden.

Ein wettbewerbsfördernder Effekt der Datenschutzgütesiegel ist fraglich. Es ist deshalb auch zweifelhaft, ob die Möglichkeit, das Gütesiegel zu Marketingzwecken zu nutzen, überhaupt in einem sinnvollen Verhältnis zu den Kosten der Prüfung stehen kann. Die Einschätzung, dass auf Seiten der Verbraucher eine Nachfrage bzw. ein

Stellungnahme

Bundesdatenschutzauditgesetz

Seite 2

entsprechender Bedarf besteht, teilen wir nicht. Diese Einschätzung ist unseres Wissens nach auch noch nirgendwo nachprüfbar belegt worden.

Allenfalls könnte in einzelnen Konstellationen ein Interesse gewerblicher Kunden bestehen, also im sog. Verhältnis B2B. Dieser Aspekt findet in der Entwurfsbegründung jedoch keinerlei Erwähnung. Hier besteht auch die Gefahr einer übermäßigen Belastung gerade kleiner und mittlerer Unternehmen.

Aufgrund der aufgezeigten Problemkreise und unserer Erfahrungswerte (zum Beispiel mit ISO-Zertifizierungen) erscheint es uns sehr fraglich, ob sich durch die Einführung eines Datenschutzaudits ein darauf basierendes Gütesiegel tatsächlich als Wettbewerbsvorteil und Nutzen für die Unternehmen etablieren wird. Ein greifbarer Nutzen für die Unternehmen könnte allenfalls in der Weise erreicht werden, dass die Auditierung und Zertifizierung für das Unternehmen mit unmittelbaren Erleichterungen oder Entlastungen bei der datenschutzrechtlichen Einbettung gekoppelt ist (z.B. beim konzerninternen Datentransfer oder beim Datentransfer in nicht sichere Drittstaaten, wenn der Prozess auditiert ist).

Schließlich sollte auch das Datenschutzaudit nicht zu einer Schwächung der Position betrieblicher Datenschutzbeauftragter führen, sondern vielmehr zu deren Stärkung, so dass deren aktive Einbindung in den Zertifizierungsprozess sichergestellt sein sollte, um den Eindruck zu vermeiden, dass die Funktion des betrieblichen DSB überprüft wird. Denkbar wäre dies durch eine weitgehend unternehmensinterne Vorbereitung und Dokumentation von Prüfungen, die vom Sachverständigen dann stichpunktartig überprüft würden.

Nach Auffassung des BITKOM ist daher vor allem gesetzgeberische Zurückhaltung und Augenmaß geboten.

Ziel des Ausführungsgesetzes zum Datenschutzaudit kann es nur sein, ein schlankes, begrenztes, praxisorientiertes und für die Unternehmen akzeptables Verfahren einzuführen. Das gewählte einstufige Verfahren ist ein erster wesentlicher Schritt, zumal die meisten Aufsichtsbehörden der Länder personell gar nicht für eine intensive Rolle im Verfahren ausgestattet sind. Dieses sollte berücksichtigen, dass eine breite Akzeptanz und ein offensichtlicher Bedarf derzeit für die Unternehmen -sofern sie ihr Kerngeschäft nicht unter Nutzung sensibler Daten betreiben- nicht ersichtlich ist.

2. Im Einzelnen: Die Inhalte des Entwurfs

Ungeachtet der oben geschilderten grundsätzlichen Bedenken wird im Folgenden auf den Anwendungsbereich und die inhaltliche Ausgestaltung der einzelnen Vorschriften des Entwurfs eingegangen.

Wir müssen jedoch darauf hinweisen, dass eine umfassende und vollständige Einschätzung der zukünftigen Situation anhand des vorliegenden Entwurfs nicht möglich ist, da wichtige Teilbereiche (insbesondere Form und Verfahren der Auditierung sowie die Einzelheiten der Antragstellung) gemäß § 8 der späteren Regelung durch Rechtsverordnungen überlassen bleiben.

2.1 Gegenstand des Audits

Gegenstand des Audits können gemäß § 1 Abs. 1 des Entwurfs ein Datenschutzkonzept sowie technische Einrichtungen der beantragenden Stelle sein.

Stellungnahme

Bundesdatenschutzauditgesetz

Seite 3

Durch diese Terminologie wird das BDSAuditG unmittelbar mit § 9a BDSG verzahnt. Diese Lösung ist nach Ansicht des BITKOM sinnvoll. Der Umstand, dass weder das BDSG noch das BDSAuditG eine Legaldefinition des „Datenschutzkonzepts“ und der „technischen Einrichtung“ geben, steht dem nicht entgegen, da ggf. derartige Definition auch im Verordnungswege (gemäß § 8 Nr. 1 bzw. 2) formuliert werden könnten. Wir regen jedoch an, dass entweder mit dem Gesetzestext oder aber in den Verordnungen ausdrücklich klargestellt wird, dass auch Verfahren und Produkte mögliche Auditgegenstände sein können, da sich dies nicht ohne Weiteres aus den Begriffen „Datenschutzkonzept“ und „technische Einrichtung“ ergibt.

Aus Sicht der Wirtschaft ist es unerlässlich, dass der Gegenstand des Audits flexibel und individuell zu bestimmen ist. Nur so kann ein angemessenes Verhältnis von Aufwand und Nutzen sichergestellt und der unternehmensspezifischen Situation Rechnung getragen werden. Das Konzept, das § 1 des Entwurfs zugrunde liegt, findet deshalb unsere Unterstützung. Wir regen jedoch an, nicht nur in der Begründung, sondern auch im Gesetz klarzustellen, dass der Umfang des Audits der Dispositionsfreiheit des Antragstellers unterliegt und daher z.B. auf Teile der Organisation oder einzelne Einrichtungen oder Produkte beschränkt sein kann.

§ 1 Abs. 3 des Entwurfs legt fest, dass sich die Bewertung nicht auf die Sicherheit informationstechnischer Systems und Komponenten erstreckt. Wir weisen darauf hin, dass diese Abgrenzung in manchen Fällen in der Praxis Schwierigkeiten bereiten könnte, zumal durch § 9 BDSG Überschneidungen angelegt sind. In § 1 Abs. 1 und § 3 Abs. 1 bis 4 BDSAuditG-Entwurf werden ausdrücklich die technischen Einrichtungen als Gegenstand eines Audits erwähnt. Hier sehen wir einen Widerspruch zur Aussage in § 1 Abs. 3 des Entwurfs.

2.2 Maßstab des Audits

Als Maßstab der Auditierung legt § 1 die „Vereinbarkeit mit den Vorschriften über den Datenschutz“ fest. Diesen Maßstab halten wir für sachgerecht. Nach unserem juristischen Verständnis des Begriff „Vereinbarkeit“ liegt eine solche auch dann vor, wenn bei ausfüllungsbedürftigen bzw. auslegungsfähigen Datenschutzvorschriften im Sinne des § 1 Abs. 2 die Vertretbarkeit bzw. Verhältnismäßigkeit gewahrt ist.

Wir gehen darüber hinaus davon aus, dass die Entwurfsverfasser die Vereinbarkeit des Maßstabs mit den Grundsätzen des UWG sichergestellt haben (§ 5 UWG, Irreführung durch Werbung mit Selbstverständlichkeiten).

2.3 Verfahren

Das mit dem Entwurf gewählte einstufige Verfahren ist dem zweistufigen Modell uneingeschränkt vorzuziehen. Für die Ausgestaltung als einstufiges Verfahren sprechen auch die bisherigen Erfahrungen mit der Zertifizierung von Qualitäts-Umwelt-, Sicherheitsmanagementsystemen (ISO 9001, 140001, 270001), bei denen es sich um von der Industrie anerkannte, seit langen praktizierte einstufige Verfahren handelt.

Nach Auffassung des BITKOM ist von zentraler Wichtigkeit, dass es bei dem gesamten Verfahren zu keinerlei unterschiedlichen Anforderungen und Rechtsfolgen kommt. Wenn Datenschutz durch ein Gütesiegel ausgewiesen werden soll, dann kann ein solches Gütesiegel nur ein einheitliches und bundesweit greifendes

Stellungnahme

Bundesdatenschutzauditgesetz

Seite 4

Gütesiegel sein. Regionale, lokale oder sektorale Einzellösungen sind für die Wirtschaft inakzeptabel. Wir begrüßen daher die Regelung in § 9 des Entwurfs und die entsprechenden Passagen in der Entwurfsbegründung.

2.4 Bestellung und Auswahl des Sachverständigen

Wir halten eine Regelung für erforderlich, nach der der Sachverständige zwar nur durch eine einzige Aufsichtsbehörde bestellt wird, aber bundesweit tätig sein darf. Zuständig für die Bestellung sollte (wie im bisherigen Entwurf) die Aufsichtsbehörde für nicht-öffentliche Stellen sein, die nach der Hauptniederlassung des Sachverständigen örtlich zuständig ist. Zudem sollte das freie Wahlrecht, das § 2 Abs. 2 S. 2 bislang nur für ausländische Antragsteller vorsieht, auch für inländische Unternehmen gelten.

§ 2 Abs. 2 des Entwurfs in seiner jetzigen Fassung hat zur Folge, dass die Freiheit bei der Auswahl des Sachverständigen durch die lokale Bindung erheblich eingeschränkt wird, da nur ein Sachverständiger beauftragt werden kann, der von der zuständigen Aufsichtsbehörde bestellt worden ist. Wir halten diese Regelung für missglückt.

Ein freies Wahlrecht würde zum Beispiel den Unternehmen, die in unterschiedlichen Bundesländern aktiv sind, die erforderliche Flexibilität ermöglichen. In diesen Konstellationen muss es möglich sein, dass die Unternehmen unabhängig vom Sitz der jeweiligen Niederlassung den gleichen Sachverständigen beauftragen. Wichtig ist dies, um die Auditierungen effizient durchzuführen zu können, Kosten zu sparen und die Einheitlichkeit der Zertifikate sicherzustellen. Auf die Notwendigkeit, der länderübergreifenden Wirtschaftstätigkeit keine störenden Schranken entgegenzusetzen, weist auch die Begründung des Entwurfs (unter II.) hin.

Sollte das von der Wirtschaft bevorzugte Modell, nach dem ein einmal bestellter Sachverständiger bundesweit tätig sein kann, nicht umgesetzt werden können, müsste zumindest sichergestellt werden, dass sich ein Sachverständiger, der schon durch eine Aufsichtsbehörde bestellt worden ist, bei einer weiteren Bestellung auf ein wesentlich erleichtertes Zulassungsverfahren berufen kann.

Nicht nur vor diesem Hintergrund müssten die Kriterien für die Akkreditierung bzw. Bestellung der Sachverständigen durch die Länder bundesweit einheitlich sein. Unterschiedliche Anforderungen in den Ländern sollten unbedingt vermieden werden.

2.5 Freiwilligkeit des Audits

Jedes Datenschutzaudit muss freiwillig sein. BITKOM begrüßt daher, dass der Entwurf in § 1 Abs. 1 die Freiwilligkeit zugrunde legt.

Wichtig ist es uns, nachdrücklich darauf hinzuweisen, dass diese Freiwilligkeit keinesfalls durch die Einbeziehung der Zertifizierung als Kriterium bei der Vergabe von Aufträgen durch die öffentliche Hand faktisch unterlaufen werden darf. Eine derartige Verbindung des Datenschutzgütesiegels mit der öffentlichen Auftragsvergabe würde die Freiwilligkeit einer Prüfung für die überwiegende Anzahl der Unternehmen illusorisch machen. Letztlich läge darin ein massiver faktischer Eingriff in den Wettbewerb.

Stellungnahme

Bundesdatenschutzauditgesetz

Seite 5

2.6 Gültigkeit der Zertifizierung und erneute Zertifizierung

2.6.1 Regelfrist

§ 3 Abs. 2 des Entwurfs legt fest, dass ein Datenschutzauditsiegel längstens zwei Jahre verwendet werden darf. In der Begründung findet sich dazu die Erklärung, dass diese Befristung erforderlich sei, da spätestens nach zwei Jahren überprüft werden müsse, ob die Vereinbarkeit weiterhin vorliegt bzw. ob zwischenzeitlich erhebliche Änderungen der Datenschutzvorschriften eingetreten sind. Soweit die Begründung sich auf die Überprüfung der weiterhin gegebenen Vereinbarkeit bezieht, überzeugt sie nicht. Denn für den Fall, dass die ursprünglich gegebene Vereinbarkeit wegen einer Veränderung der zertifizierten Version fraglich geworden ist, sieht § 3 Abs. 2 ein eigenes Verfahren vor. Unter dem Aspekt der erheblichen Änderung der datenschutzrechtlichen Vorschriften aber ist die Regelbefristung auf zwei Jahre nach Auffassung des BITKOM willkürlich gewählt und viel zu kurz. Damit eine Auditierung für die Unternehmen attraktiv und lohnenswert ist, müsste die Regelbefristung mindestens vier Jahre betragen. In die Beurteilung ließe sich gegebenenfalls der betriebliche Datenschutzbeauftragte einbinden, dem die Aufgabe zugewiesen werden könnte, bestehende Zertifizierungen auf wesentliche Änderungen hin zu überwachen, womit auch seine innerbetriebliche Rolle gestärkt würde.

2.6.2 Erneute Zertifizierung und Bezugsgegenstand der Zertifizierung

§ 3 Abs. 2 des Entwurfs hat zur Folge, dass das Datenschutzauditsiegel nur für das Produkt (Technische Einrichtung) oder das Konzept gültig ist, das dem Sachverständigen baugleich oder textidentisch als Prüfmuster vorgelegen hat. Wird das Produkt bzw. das Konzept gegenüber dem evaluierten Prüfmuster verändert, muss das Verfahren erneut durchgeführt und eine Zertifizierung beantragt werden. Eine wie auch immer geartete Erheblichkeitsschwelle ist nicht vorgesehen. Diese Anforderung geht vollständig an der Wirklichkeit und Erforderlichkeit schneller Produkt- und Verfahrenszyklen bzw. Verbesserungen der ITK-Industrie vorbei, in der erfahrungsgemäß der Lebenszyklus unveränderter Produkte in Monaten gemessen wird. Sie wird häufig dazu führen, dass ein Produkt, für das das Zertifizierungsverfahren noch nicht abgeschlossen ist, schon zugunsten seines Nachfolgers vom Markt genommen wurde. Eine derartige Regelung trägt zur Innovationsfeindlichkeit des Standortes Deutschland bei, bremst technische Entwicklung und ignoriert die Bedürfnisse der vorrangig betroffenen Branche. In den Unternehmen dürfte diese Regelung häufig zu einer Entscheidung gegen eine Zertifizierung führen, da das Verfahren unattraktiv und unpraktikabel ist.

Wir regen daher nachdrücklich an, die gesamte Regelung der Befristung und wiederholten Zertifizierung neu zu gestalten. Die folgenden Regelungselemente sollten in einer Neuformulierung des § 3 Abs. 2 berücksichtigt werden:

- Bei unveränderter Version/unverändertem Konzept ist nach dem Ablauf der Regelfrist ein erheblich vereinfachter Re-Zertifizierungsprozess erforderlich. Entscheidend sollte die Selbsteinschätzung des Antragstellers sein, die ggf. durch eine vom Sachverständigen durchzuführende, vereinfachte Begutachtung ergänzt wird.
- Bei veränderter Version/verändertem Konzept: Sind vom Antragsteller Veränderungen vorgenommen worden, muss zwischen

Stellungnahme

Bundesdatenschutzauditgesetz

Seite 6

datenschutzrelevanten und -irrelevanten Veränderungen unterschieden werden. Maßgeblich sollte auch hier die Selbsteinschätzung des Antragstellers sein, die ggf. durch eine vom Sachverständigen durchzuführende, vereinfachte Begutachtung ergänzt wird.

- Der Begriff der „zertifizierten Version“ müsste präzisiert werden.

Ein derart gestaltetes Verfahren würde auf Seiten der betroffenen Unternehmen die Akzeptanz und Attraktivität einer Zertifizierung erheblich fördern. Zudem würde der Verwaltungsaufwand bei der Registerführung stark verringert. Der Wert der Zertifizierung würde durch die Selbsteinschätzung auch nicht in Frage gestellt, wenn bei einer unzutreffenden Selbsteinschätzung § 5 und die Sanktionsvorschriften § 6 und § 7 greifen. Ist der Antragsteller im Zweifel darüber, ob eine relevante Veränderung vorliegt, bleibt ihm eine Vorabanfrage bei der Aufsichtsbehörde bzw. bei einem zugelassenen Sachverständigen unbenommen.

2.8 Transparenz für den Kunden

Die Möglichkeit, das Datenschutzauditregister für Jedermann im Internet einsehbar zu machen, halten wir für eine sachgerechte Lösung, die die notwendige Transparenz und Orientierung sicherstellt.

2.9. Verwaltungsverfahren

An manchen Stellen des Entwurfs bleibt die Einbindung der Vorschriften in das allgemeine Verwaltungsrecht noch unklar, wir regen daher an, den Entwurf insoweit noch einmal zu prüfen.

2.10 Sonstiges

Nicht nur dort, wo Produkte oder Systeme vom Nutzer individuell konfiguriert werden können, hat der Hersteller wenig Einfluss auf die Art und Weise des tatsächlichen Produkt- bzw. Systemesinsatzes. Es muss daher die Frage aufgeworfen werden, ob es wirklich sinnvoll ist, die Verantwortlichkeit für den Datenschutz umfassend in die Sphäre des Herstellers zu verlagern. Denn der Hersteller kann höchstens die Voraussetzungen für einen datenschutzgerechten Einsatz schaffen, die Erfüllung dieser Voraussetzungen und datenschutzrechtlichen Anforderungen liegt letztlich jedoch allein in der Hand des jeweiligen Anwenders. Der Nutzer muss daher für einen datenschutzgerechten Einsatz von Produkten sensibilisiert und zu einem verantwortungsbewussten Umgang befähigt werden.

Ähnlich liegt das Problem in den häufigen Konstellationen, dass das Produkt oder System nicht isoliert, sondern als eine von vielen Komponenten eines Gesamtsystems zum Einsatz kommt. Auch hier ist das Zusammenspiel der Komponenten und dessen datenschutzrechtliche Konformität dem Einfluss des einzelnen Herstellers entzogen.