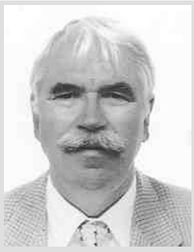
DuD
Datenschutz und Datensicherheit

Datenschutzaudit – Quo Vadis ?

Uwe Dieckmann, Bernd Eitschberger, Harald Eul,
Paul Schwarzhaupt, Gerwald Wohlrab

Das neue BDSG ist nunmehr in Kraft. Ein sehr konträr diskutierter Abschnitt des neuen BDSG war das Datenschutzaudit. Dieser Beitrag diskutiert wie ein Datenschutzaudit möglichst unbürokratisch und mit vernünftigem Aufwand umgesetzt werden kann und appelliert an den Gesetzgeber, dies bei der Entwicklung des Ausführungsgesetzes zu berücksichtigen.



Dipl.Kfm.
Uwe Dieckmann

Leiter Revision und betrieblicher DSB bei Wüstenrot Bausparkasse AG

E-Mail: uwe.dieckmann@wuestenrot.de

Dr.
Bernd Eitschberger

Leiter Sicherheit und betrieblicher DSB bei Veba Oil Refining & Petrochemiclas GmbH

E-Mail: bernd.eitschberger@vorp.de

Harald Eul

Unternehmensberater für Datenschutz und Datensicherheit sowie externer DSB

E-Mail: H.Eul@HE-C.de

1 Einleitung

Im neuen BDSG ist formuliert, dass „Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen prüfen und bewerten lassen... „ können.

Im Zuge des Gesetzgebungsverfahrens ist dieser Paragraf mehrfach geändert, verworfen und modifiziert worden. Schließlich ist er in seiner ursprünglichen Entwurfsform im verabschiedeten Gesetz wieder enthalten.

2 Datenschutzaudit umstritten

Nach einer Umfrage im GSE-Arbeitskreis Datenschutz und Datensicherheit[1] sprechen sich die Datenschutzbeauftragten großer Teile der Wirtschaft gegen ein Datenschutzaudit aus.[2]

Paul Schwarzhaupt

Betrieblicher DSB bei R+V Versicherungs- Gruppe

E-Mail: Paul.Schwarzhaupt@RUV.de

Dipl. Math.
Gerwald Wohlrab

Betrieblicher DSB bei Amadeus Data Processing GmbH
E-Mail: Gwohlrab@amadeus.net

[1] Die Autoren bilden die Arbeitsgruppe Datenschutzaudit des GSE-(Guide Share Europe)-Arbeitskreises Datenschutz und Datensicherheit. Im Arbeitskreis sind 65 deutsche Unternehmen durch ihre Datenschutz- bzw. Datensicherheitsexperten vertreten.

Die wesentlichen Bedenken stammen insbesondere aus folgenden Problemkreisen:

- Schlechte Erfahrungen (Bürokratisierung) mit dem Qualitätsaudit nach ISO DIN EN 9000 ff. und wenig Qualitätssteigerung aus Sicht des Verbrauchers
- Fragliches Kosten-Nutzen-Verhältnis
- Dreifache Kontrolle der Unternehmen durch DSB, Aufsichtsbehörde und Zertifizierer mit Unklarheit der Zuständigkeiten (Unabhängigkeit und Weisungsfreiheit des DSB, unklare Rechtsbeziehungen zwischen Aufsicht und Zertifizierer)[3]

Da im neuen BDSG ein Datenschutzaudit aufgenommen wurde, muss diesen durchaus berechtigten Bedenken unbedingt durch das erforderliche Ausführungsgesetz Rechnung getragen werden. Unter dieser Voraussetzung bliebe dann als grundlegendes Problem, ob ein Datenschutzaudit für alle datenverarbeitenden Stellen oder nur für Anbieter von DV-Systemen und Programmen gefordert werden soll. Bisher ist in der Diskussion allerdings zu kurz gekommen, dass es Unternehmen (datenverarbeitende Stellen) gibt, die ihr Kerngeschäft nur unter Nutzung sensibler Kundendaten betreiben und ein Datenschutzaudit als Wettbewerbsvorteil verwenden können.

3 Ökoaudit Vorbild für Datenschutzaudit?

Eines der Kernprinzipien des mit einem Gütesiegel versehenen Audits soll nach bisher bekannt gewordenen Plänen die kontinuierliche Verbesserung des Datenschutzniveaus sein. Danach soll eine Zertifizierung zunächst ein über dem gesetzlichen Mindeststandard liegendes Datenschutzniveau voraussetzen. Eine wieder-

[2] Vgl. u.a. Hans-Ludwig Drews, Hans Jürgen Kranz Datenschutzaudit, DuD 02/2000, 226

[3] Vgl Gola, Der auditierte Datenschutzbeauftragte – oder von der Kontrolle der Kontrolleure, RDV 03/2000, 93

holte bzw. nachfolgende Auditierung soll jedoch nach Aussagen des von Professor Roßnagel für das Bundeswirtschaftsministerium erstellten Gutachtens nur dann zu einem Gütesiegel rechtfertigen, wenn gegenüber dem vorherigen Audit das Datenschutzniveau angehoben wurde. [4]

Die Zielsetzung einer kontinuierlichen Verbesserung stößt jedoch einvernehmlich auf massive Bedenken. Die vom Ökoaudit (EMAS) abgeleitete kontinuierliche Verbesserung ist auf den Datenschutz nicht übertragbar. Im Umweltschutz ist für jedermann wünschenswert, dass umweltbelastende Immissionen nicht nur reduziert sondern, letztlich verhindert werden sollten. Man mag einwenden, dass eine derartig auf die Spitze getriebene Umweltpolitik die Unternehmen ruinieren könnte. Damit wird jedoch eine Diskussion eröffnet, deren Argumente sehr von politischen Überzeugungen geprägt sind.

Allerdings kann im Bereich der Datensicherheit das Prinzip der kontinuierlichen Verbesserung sinnvoll sein. Zum einen gibt es hier keinen absoluten Wert, der z. B. aus einer Gesetzesvorschrift ableitbar wäre. Spielraum für kontinuierliche Verbesserungen ergibt sich dabei naturgemäß dadurch, dass die vom jeweiligen Unternehmen selbst gesetzte Zielgröße regelmäßig deutlich über dem aktuellen Status der erreichten Sicherheitsstandards liegt und üblicherweise nur in längerfristigen Veränderungsprozessen erreicht werden kann. Dies in verschiedenen Stufen anzugehen, die durch jeweils ein (z. B. jährliches) Audit gekennzeichnet sind, macht Sinn und würde einen kontinuierlichen Verbesserungsprozess in Gang setzen. Der Spielraum für Verbesserungen ergibt sich im Bereich der Datensicherheit aber auch dadurch, dass das jeweilige Unternehmen den Umfang der Schutzbedürftigkeit der Unternehmensdaten erweitert und damit die Zielgröße für das wünschenswerte Sicherheitsniveau setzt. Und schließlich werden aufgrund der Komplexität der Datenverarbeitungssysteme, der permanenten Weiterentwicklung sowie der „Innovationsgeschwindigkeit“ bei den Sicherheitsgefährdungen (z. B. neue Viren oder sonstige Angriffsformen) die Anforderungen an die Datensicherheit ständig erweitert. Um ein definiertes Sicherheitsniveau zu gewährleisten, müssen daher die entsprechenden Sicherheitsmaßnahmen permanent verbessert werden. Somit ist ein kontinuierlicher Verbesserungsprozess im Zusammenhang mit der Datensicherheit nicht nur sinnvoll sondern, systemimmanent. Anders aber beim Datenschutz.

Im Bereich Datenschutz würde eine kontinuierliche Verbesserung irgendwann einmal dazu führen, auf die Verarbeitung von personenbezogenen Daten zu verzichten. Dies würde zum Wegfall der Geschäftsgrundlage und damit zwangsläufig zur Einstellung des Geschäftsbetriebes führen müssen. Es muss auch beachtet werden, dass das informationelle Selbstbestimmungsrecht nicht absolut ist, sondern Schranken zugunsten der Allgemeinheit hingenommen werden müssen. Die Vielzahl vorrangiger, den Datenschutz einschränkender Gesetze, aber auch die Möglichkeit der Einwilligung des Betroffenen machen ein Datenschutzaudit nicht vergleichbar mit dem Ökoaudit. Die kontinuierliche Verbesserung des Datenschutzes im Sinne der von Roßnagel in seinem Gutachten vorgeschlagenen Grundlagen für ein Audit könnte daher für ein einzelnes Unternehmen nur für einen beschränkten Zeitraum funktionieren. Nach Roßnagel soll aber eine erneute Zertifizierung nur dann erfolgen können, wenn gegenüber dem letzten Audit eine Verbesserung erreicht wurde.

Wenn aber das Unternehmen dann das optimale und kundenfreundlichste Datenschutzniveau erreicht hat und eine weitere Verbesserung ohne Gefährdung des Geschäftsbetriebes nicht mehr möglich ist, würde jedoch eine weitere Zertifizierung des Unternehmens versagt werden. Der von Roßnagel erwünschte wettbewerbsstimulierende Effekt einer Datenschutzzertifizierung würde in dem geschilderten Fall sich gegen das Unternehmen richten: Genau zum Zeitpunkt größter Wettbewerbsfähigkeit im Datenschutz würde das Gütesiegel mangels der Möglichkeit einer weiteren Verbesserung des Datenschutzes zurückgezogen werden. Ein paradoxes Ergebnis.

Deshalb kann die kontinuierliche Verbesserung des Datenschutzes nicht analog des Ökoaudits Grundlage des Datenschutzaudits sein.

[4] Roßnagel, Datenschutzaudit, Konzept und Entwurf eines Gesetzes für Datenschutzaudit, Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie

4 Datenschutzaudit – Zertifizierung der Gesetzeskonformität ?

Die Alternative wäre, ein Audit ausschließlich auf die Frage der Erfüllung der gesetzlichen Anforderungen durch das Unternehmen zu beschränken. Wie das am Beispiel eines Unternehmens, das die gesetzlichen Anforderungen noch nicht erfüllt (Abb. 1), verdeutlicht wird, würden von einem Datenschutzaudit durchaus Impulse für die Erfüllung der gesetzlichen Anforderungen ausgehen. Bereits die Vorbereitung auf ein Audit führt zu einer breiten Sensibilisierung der Mitarbeiter und zu entsprechenden Veränderungs- bzw. Verbesserungsprozessen, deren Dynamik einige Zeit nach der Durchführung eines Audits allerdings nachlassen dürfte. Solange jedoch die gesetzlichen Anforderungen nicht vollständig umgesetzt sind, dürfte auch keine Zertifizierung erfolgen.

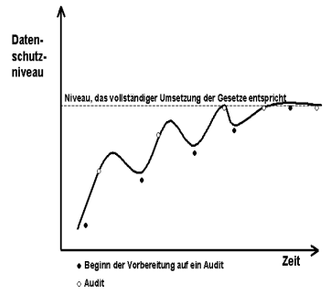


Abb. 1: Erfüllung gesetzlicher Normen

Was wäre aber von einem Zertifikat über die Erfüllung der gesetzlichen Anforderungen zu halten?

Obwohl es Beispiele im Wirtschaftsleben gibt, bei denen die Erfüllung gesetzlicher oder anderer Normen auditiert und zertifiziert werden (z. B. TÜV-Plakette bei Kraftfahrzeugen, CRS-Audit bei Flugbuchungssystemen), würde ein derart beschränktes Datenschutzaudit folgende Negativeffekte zur Folge haben:

1. Verbürokratisierung
2. unnötige Kosten
3. faktischer Zwang für alle Unternehmen, da ein fehlendes Zertifikat implizieren würde, dass das Unternehmen die gesetzlichen Anforderungen nicht erfüllt.

Eine Beschränkung des Audits auf die Einhaltung der gesetzlichen Anforderungen kann daher nicht unterstützt werden.

5 Datenschutzaudit – ja oder nein ?

Nach Meinung der Arbeitskreisteilnehmer ist ein Datenschutzaudit nicht überflüssig, weil es eine sinnvolle Alternative gibt: Ein Audit, das ein über die gesetzlichen Anforderungen hinausgehendes Datenschutzniveau zertifiziert, nicht aber eine kontinuierliche Verbesserung verlangt. Das schließt nicht aus, dass aus Unternehmens- bzw. Marketingüberlegungen wegen des Wettbewerbs weitere Verbesserungen des Datenschutzes im Zeitablauf vorgenommen werden.

Gegenstand des Audits und damit des entsprechenden Gütesiegels wäre aber immer der aktuelle Status, über dessen Kunden-/Verbraucherorientiertheit letztlich der Konsument im Hinblick auf seine spezifischen Bedürfnisse sowie im Vergleich zum Wettbewerb entscheidet. Siehe dazu Abb. 2.

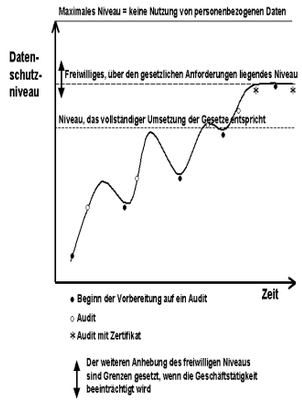


Abb. 2 Übererfüllung gesetzlicher Normen

Es gibt zahlreiche Möglichkeiten, das gesetzliche Datenschutzniveau zu überschreiten. Das liegt einerseits daran, dass die technischen und organisatorischen Datensicherungsmaßnahmen stets daraufhin beurteilt werden müssen, ob der damit verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Auf der anderen Seite sind auch die Grundsätze der Datensparsamkeit, Maßnahmen zur Anonymisierung oder Pseudonymisierung individuell ausgestaltbar. Auch Art und Weise, wie ein Unternehmen die Betroffenen über die Datenverarbeitung und ihre Rechte informiert, können über das gesetzlich Geforderte hinausgehen. So können z. B. im Sinne des Verbrauchers Anstrengungen unternommen werden, die Transparenz über seine Datenschutzrechte zu verbessern. Oder das Unternehmen könnte sich zu bestimmten, datenschutzfreundlichen Maßnahmen verpflichten. Dies würde das Unternehmen in einem so genannten Datenschutzversprechen bzw. in so genannten Datenschutzprinzipien wettbewerbswirksam veröffentlichen können. Auch dieses Modell würde produkt-/service- oder sogar unternehmensbezogen Auditierungen zulassen. Wie auch die Veröffentlichung bestimmter Datenschutzprinzipien bzw. das Datenschutzversprechen sich auf Produkte und Leistungen oder auf das gesamte Unternehmen beziehen kann. Solche Modelle werden z. B. durch Truste bzw. BBB-online gefördert.[5]

6 Zentrale Rolle des betrieblichen Datenschutzbeauftragten !

Im Rahmen der Gestaltung des künftigen Ausführungsgesetzes zum Datenschutzaudit fordert der Arbeitskreis die Berücksichtigung der Einbindung der Datenschutzbeauftragten, wie nachfolgend beschrieben.

Eine zentrale Rolle bei der Datenschutz-Auditierung der Unternehmen nimmt der betriebliche oder behördliche Datenschutzbeauftragte ein. Er agiert in seiner Zuständigkeit und Verantwortung als interner Auftraggeber und Begleiter des Datenschutzaudits. Erst durch seine profunden Kenntnisse über das Unternehmen und sein ‚Insider' Wissen kann ein Datenschutzaudit sinnvoll durchgeführt werden. Der Datenschutzbeauftragte ist aufgrund der gesetzlichen Anforderungen an seine Eignung und Fachkunde der Mittler zwischen seinem Unternehmen und den externen Auditoren. Die zu erwartenden Ausbildungsseminare für externe Auditoren eignen sich in gleicher Weise auch für die Datenschutzbeauftragten, um ihr (ggf. zu auditierendes) Ausbildungsniveau auf den geforderten Stand zu bringen.

[5] www.truste.com/programs/pub_principles.html, www.bbb.org/

7 Unternehmens- oder verfahrensorientierte Zertifizierung ?

Weiterhin ist zu berücksichtigen, dass nicht die Gesamtheit aller DV-Prozesse bei der datenverarbeitenden Stelle einem Datenschutzaudit unterliegen können. Diese Auditierungen würde bei vielen Unternehmen nicht ökonomisch sein. Aus der Vielzahl der DV-Prozesse sind sinnvolle Teilprozesse zu selektieren; diese können dann auditiert werden.

Die Selektion sollte der datenverarbeitenden Stelle oder ihren Dachverbänden überlassen bleiben. Auswahlkriterium ist dabei die Sensibilität der personenbezogenen Datenverarbeitungsprozesse. Anhaltspunkte für die Sensibilität von Datenverarbeitungen gibt das Gesetz (z. B. § 28 Abs. 2 und Abs. 6-8 oder § 39 BDSG). Auch die in § 4 d Abs. 5 des BDSG angesprochenen „besonderen Risiken für die Rechte und Freiheiten der Betroffenen" bei bestimmten Verarbeitungen, die der Vorabkontrolle bedürfen, zählen dazu.

Es macht Sinn, eine Einteilung nach den Personengruppen vorzunehmen, deren Daten verarbeitet werden. Angenommen, man entscheidet sich für ein Audit aus Wettbewerbsgründen, ist die wichtigste Personengruppe die der Kunden und ggf. der Interessenten. Der Auftrag für ein Audit beschränkt sich dann auf die Verarbeitungsprozesse, zu deren Zweck ein Unternehmen die Daten erhalten hat und natürlich darauf, ob sichergestellt ist, dass keine zweckfremden Verarbeitungen oder wenn überhaupt, dann nur im Rahmen von vorrangigen Rechtsvorschriften oder mit der Einwilligung der Betroffenen vorgenommen werden.

Es wäre also denkbar, dass ein Unternehmen lediglich ein Zertifikat bekommt für die Einhaltung der Datenschutzvorschriften im Zusammenhang z. B. mit

- Antragsbearbeitung, Kontoführung und Darlehensverwaltung (bei Banken)
- Antragsbearbeitung und Vertragsverwaltung bei Lebensversicherungen
- Abwicklung von E-Commerce-Aufträgen über das Internet (Versandhandel)
- Auftragsdatenverarbeitung (Rechenzentrum)
- Ordnungsgemäße Datenträgervernichtung (Entsorgungsunternehmen)

- Erhebung und Verarbeitung von Befragungsdaten (Markt- und Meinungsforschungsinstitute)

In einem ganz anderen Zusammenhang sind die Geschäftsprozesse zu sehen, welche Mitarbeiterdaten betreffen. Hier steht wohl kaum der Wettbewerbsgedanke im Vordergrund, sondern eher der Druck von Arbeitnehmerinteressenvertretungen und Datenschutzbeauftragten. Im Gegensatz zum Bereich der Verarbeitung von Kundendaten wird in den meisten Fällen Standardsoftware eingesetzt. Auch die vielen gesetzlichen Übermittlungsvorschriften lassen es nicht sinnvoll erscheinen, ein Datenschutzaudit der gesamten Datenverarbeitung inklusive der auf die Mitarbeiter bezogenen Systeme durchzuführen.

8 Ist ein Gütesiegel allein aussagefähig ?

Das Ergebnis des Datenschutzaudit kann nicht in der Frage „Gütesiegel ja oder nein?" enden. Da das Audit eine Beurteilung ermöglichen soll, inwieweit der Datenschutz über gesetzliche Anforderungen hinausgeht, ist eine Klassifizierung der Beurteilung (Ranking) die zwangsläufige Folge.

Wie sich aus Abb. 2 ergibt, ist die Einhaltung der gesetzlichen Anforderungen ein unbedingtes Muss für eine Zertifizierung. Es gibt aber auch Unternehmen, die bereits Standards im Rahmen einzelner Verarbeitungen einhalten, die manchmal schon weit über dem durch die Gesetze geforderten Niveau liegen. Insbesondere dort, wo nicht nur die Datengeheimnisse der Betroffenen, sondern allgemein auch Betriebsgeheimnisse geschützt werden müssen, ist das Gesetzesniveau überschritten. Es wäre nicht sachgerecht, hier lediglich eine „TÜV-Plakette" zu verleihen. Der Bürger kennt nicht die Qualität der Datenschutzgesetze mit den vielen Ausnahmen und Abwägungsmöglichkeiten. Er vermutet, dass seine Daten bei den Unternehmen zweckentsprechend verarbeitet werden. Er ahnt nicht, dass z. B. ein unter das TKG fallendes Unternehmen trotz Schnittstelle zum Geheimdienst ein Gütesiegel bekommen kann. Dies trifft insbesondere dann zu, wenn vermehrt auch internationale Kundschaft, die diese Gesetze nicht kennt, betroffen ist. Gesamturteile sind immer kritisch, wenn man nicht weiß, aus welchen einzelnen Prüfungskomponenten sich diese ergeben. So sind i. d. R. Bestätigungsvermerke von Wirtschaftsprüfern ohne die Kenntnis des Prüfungsberichts ebenso wertlos wie ein Gesamturteil bei Warentests ohne die Kenntnis der einzelnen Bewertungsmaßstäbe. Deshalb sollten insbesondere die Risiken einzelner Verarbeitungen (meist branchenbezogen) erläutert und die zur Risikominimierung durchgeführten Maßnahmen bewertet werden. Das auditierte Unternehmen hätte dann die Möglichkeit, mit diesen Ergebnissen an die Öffentlichkeit zu gehen.

9 Fazit

Da der Gesetzgeber nun das Datenschutzaudit etabliert hat, ist der Fokus auf eine sinnvolle Ausgestaltung zu legen.

Ein kontinuierlicher Verbesserungsprozess im Zusammenhang mit der Datensicherheit ist systemimmanent. Anders aber beim Datenschutz. Deshalb kann die kontinuierliche Verbesserung des Datenschutzes nicht analog des Ökoaudits Grundlage des Datenschutzaudits sein. Eine Beschränkung des Audits auf die Einhaltung der gesetzlichen Anforderungen kann ebenfalls nicht unterstützt werden.

Daher wird ein Audit vorgeschlagen, das ein über die gesetzlichen Anforderungen hinausgehendes Datenschutzniveau zertifiziert, nicht aber eine kontinuierliche Verbesserung verlangt.

Bei der bisherigen Diskussion, ob ein Datenschutzaudit bei Dienstleistern oder allen datenverarbeitenden Stellen in Betracht kommt, wurde übersehen, dass es Unternehmen gibt, die ihr Kerngeschäft nur unter Nutzung sensibler Kundendaten betreiben und ein Datenschutzaudit als Wettbewerbsvorteil verwenden können. Eine Unterteilung in die Gruppe der Dienstleister, Anbieter von DV-Systemen und -programmen sowie datenverarbeitende Stellen mit besonders sensiblen Verfahren einerseits gegenüber den übrigen Stellen andererseits wird empfohlen. Die erste Gruppe könnte für ein Datenschutzaudit in Frage kommen.

Nicht die Gesamtheit aller DV-Prozesse bei dem zu zertifizierenden Unternehmen müssen einem Datenschutzaudit unterliegen. Ein Gesamtaudit erscheint in den meisten Fällen ökonomisch auch nicht sinnvoll. Aus der Vielzahl der DV-Prozesse sind daher entsprechende Teilprozesse zu selektieren.

Das Audit soll eine Beurteilung ermöglichen. Der Bürger kennt nicht die Qualität der Datenschutzgesetze mit den vielen Ausnahmen und Abwägungsmöglichkeiten. Er ahnt z. B. nicht, dass ein unter das TKG fallendes Unternehmen trotz Schnittstelle zum Geheimdienst ein Gütesiegel bekommen kann. Das Gütesiegel muss Aussagen ermöglichen, die über ein „Ja" oder „Nein" hinausgehen.

Gefordert ist hier der Gesetzgeber, der jetzt ein Ausführungsgesetz zum Datenschutzaudit zu entwickeln hat. Ziel muss es sein, die durchaus positiven Aspekte eines Datenschutzaudits in ein vernünftiges, für die Unternehmen wie für die betrieblichen Datenschutzbeauftragten hilfreiches und akzeptables Auditierungsverfahren umzusetzen.

Literatur

[Bäum00] Helmut Bäumler: *Der neue Datenschutz in der Realität* DuD 5/2000 S. 260

[Bend99] Bender Rolf: *Gesetzliche Vorgaben für ein Datenschutzaudit* Vortrag DAFTA 23Forum 4

[Büll97] Büllesbach Alfred: *Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor* RDV 6/1997, S. 239-280

[Bund95] *Vierter Zwischenbericht der Enquete-Kommission – Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft* Bundesdrs. 13/11002 S. 107-109

[CWLN97] Christian Peter Wilde, Ludwig Nawa: *Mitwirkung des TÜV bei der Datenschutzaufsicht über Private* DuD 09/1997 S. 516 –519

[HDHK98] Hans-Ludwig Drews, Hans Jürgen Kranz: *Argumente gegen die gesetzliche Regelung eines Datenschutz-Audits* DuD 2/1998 S. 93 – 94

[HDHK00] Hans-Ludwig Drews, Hans Jürgen Kranz: *Datenschutzaudit (Anmerkung zum Rechtsgutachten von Alexander Roßnagel vom Mai 1999* DuD 4/2000 S. 226 – 230

[König00] Thomas Königshofen: *Chancen und Risiken eines gesetzlichen geregelten Datenschutzaudits* DuD 6/2000 S. 357-360

[Roßn99] Alexander Roßnagel: *Datenschutzaudit; Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit (Rechtsgutachten für das BMW)* www.datenschutz-help.de/audit.htm

[Roßn00] Alexander Roßnagel: *Audits stärken Datenschutzbeauftragte (Replik zum Beitrag „Datenschutzaudit" von Drews und Kranz)* DuD 4/2000 S. 231 – 232