

# Datenschutzaudit nach IT-Grundschutz – Konvergenz zweier Welten

Frank Reiländer, Gerhard Weck

*Spätestens mit der BDSG-Novelle vom Mai 2001 orientiert sich der Datenschutz immer stärker an den originären Kriterien der IT-Sicherheit, deren Bedeutung im Vergleich zu den eher juristisch geprägten Organisationsanforderungen deutlich steigt. Der Beitrag zeigt die Konvergenz von Audit-Forderungen des Datenschutzes hin zu einem bewährten, standardisierten Ansatz der IT-Sicherheit, dem IT-Grundschutzhandbuch, auf. Im Praxisteil wird geschildert, wie sich dies bereits effizient im privatwirtschaftlichen sowie öffentlichen Bereich umsetzen lässt.*



Frank Reiländer  
Dipl.-Informatiker,  
lizenzierter IT-Grundschutz-Auditor.  
Arbeitsschwerpunkte:  
Org. IT-Sicherheitsmanagement, Erstellung von Security Policies, Sicherheitsbewertungen nach IT-GSHB,

Konzeption Datenschutzaudit, Tätigkeiten als IT-Sicherheitsbeauftragter und bDSB.  
E-Mail: f.reilaender@infodas.de



Dr. Gerhard Weck  
Studium der Physik,  
lizenzierter IT-Grundschutz-Auditor.  
Arbeitsschwerpunkte:  
Sicherheit von Betriebs- und Informationssystemen, Entwicklung IT-Sicherheitsdatenbank

der Infodas. Dozent zu IT-Sicherheit bei udis, Sprecher der DECUS-Fachgruppe Security.  
E-Mail: g.weck@infodas.de

## 1 IT-Sicherheit und das BDSG

Die mit der Novellierung vom Mai 2001 verabschiedete dritte Fassung des Bundesdatenschutzgesetzes (BDSG) wurde wesentlich von zwei Faktoren getrieben: Einerseits drängte die Umsetzung der Vorgaben aus der EG-Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 [EG95]; weiterhin sollten zahlreiche Überlegungen für ein „modernes Datenschutzrecht“ ihren Niederschlag im Gesetzestext finden. Angesichts des Zeitdrucks hinsichtlich des aus der EG-Richtlinie resultierenden Termins zur Umsetzung in nationales Recht (24.10.1998), der bereits deutlich überschritten war, wurde eine grundlegende Modernisierung des Datenschutzrechts auf eine „zweite Stufe“ der Novellierung verlagert. Wichtige Eckwerte wie die dem Systemdatenschutz zuzurechnenden Prinzipien der Datenvermeidung und Datensparsamkeit, des Datenschutzes durch Technik sowie die Festschreibung eines freiwilligen Datenschutzaudits, das u. a. den Trend zur Stärkung der Selbstkontrolle verdeutlichen soll, wurden allerdings aufgenommen.

Zu weiteren Säulen der Neuregelungen zählen neben dem erweiterten Geltungsbereich und der erweiterten Transparenz gegenüber dem Betroffenen erweiterte Verarbeitungsbeschränkungen und eine erweiterte Datenschutzkontrolle. Gerade die beiden letztgenannten Kriterien führen – neben einer Stärkung der Position des betrieblichen Datenschutzbeauftragten – zu einem deutlichen Zuwachs an Pflichten und Verantwortung. Die Anforderungen an die Fachkunde des betrieblichen Datenschutzbeauftragten gemäß § 4f Abs. 2 [BDSG01] werden im Vergleich zur Fassung von 1990 [BDSG90]

inhaltlich zwar nicht konkretisiert.<sup>1</sup> Dadurch aber, dass der bDSB die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme überwachen muss und in kritischen Fällen explizit eine Vorabkontrolle durchzuführen hat, ergibt sich zwingend, dass der betriebliche Datenschutzbeauftragte sich ein umfassendes IT-Fachwissen und insbesondere auch grundlegende Kenntnisse zur IT-Sicherheit aneignen muss.

## 2 Standardisierung von IT-Sicherheit

### 2.1 Nationale und internationale Standards

In einer zunehmend stärker und engmaschiger vernetzten IT-Welt, die mittels offener Standards interagierende IT-Systeme verbindet, beschreiben die Regelwerke und IT-Sicherheitsstandards analog dazu nicht mehr das einzelne System oder gar dessen Kern, sondern basieren auf vernetzten IT-Landschaften und durch Prozesse beschriebenen Abläufen. Als Vertreter der System- bzw. Kernel-Sichtweise seien die ITSEC-Kriterien oder auch das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene IT-Grundschutzhandbuch [IT-GSHB] in seinen Versionen von 1995 bis 2000 genannt. Die Abbildung der heutigen Sicht auf die IT-Strukturen ist in die Sicherheitsstandards in unterschiedlicher Durchdringungstiefe eingeflossen, zu einem großen Teil auch abhängig davon, ob der jeweilige Standard neu konzipiert wurde oder ein etablierter Standard lediglich um aktuelle Aspekte „angereichert“ wurde. Als Vertreter der ganzheitlichen Sicht hinsichtlich organisatorischer Regelungen und der

<sup>1</sup> Es wurde lediglich konkretisiert, dass mit der Aufgabe des betrieblichen Datenschutzbeauftragten (bDSB) auch eine Person außerhalb der verantwortlichen Stelle betraut werden kann.

gesteigerten Komplexität in Bezug auf Netzstrukturen und Schnittstellen seien die Protection Profiles in den Common Criteria (CC), der „Best Practice“-Ansatz nach BS 7799 bzw. ISO 17799 sowie CobiT genannt. Durch die Einführung der Schichtenstruktur und mit Modellierung des IT-Verbunds haben Prozesse und Netze eine adäquate Abbildung im IT-Grundschutz gefunden.

## 2.2 Stellenwert des IT-Grundschutzes

Im IT-Grundschutzhandbuch finden sich Maßnahmenempfehlungen zur Erreichung eines mittleren Schutzniveaus in den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit. Sicher mag vielleicht ein wenig überholungsbedürftig klingen; dies ist jedoch der Preis für die Konkretheit der – oft bis in technische Details beschriebenen – Maßnahmenempfehlungen. Im Gegensatz zum komplexen IT-Sicherheitshandbuch aus dem Jahr 1992 lässt sich durch die Umsetzung der standardisierten Maßnahmenempfehlungen eine Basis-Sicherheit etablieren, ohne dass hierfür die Durchführung einer expliziten Risikoanalyse erforderlich ist.

Die Maßnahmenempfehlungen wurden über die Jahre so angepasst, dass sie sich auch auf Systeme mit hohem Schutzbedarf anwenden lassen. Sie bilden dabei die Basis für eine ergänzende Sicherheitsanalyse, z. B. mit Hilfe des IT-Sicherheitshandbuchs. Das IT-Grundschutzhandbuch ist somit in der Lage, den Aufbau eines IT-Sicherheitsmanagements durchgängig zu unterstützen.

Ebenso unterstützt wird der Trend zu verlässlicher Sicherheit: Die IT-Grundschutz-Methodik sieht seit Frühjahr vergangenen Jahres ein Qualifizierungs- und Zertifizierungsschema vor. Als zu zertifizierender Untersuchungsgegenstand ist der IT-Verbund definiert, „der die Fachanwendungen einer Organisationseinheit und alle hierzu benötigten informationstechnischen Komponenten umfasst“. Das IT-Grundschutz-Zertifikat stellt innerhalb des Qualifizierungsschemas den höchsten Grad der Vertrauenswürdigkeit und des Sicherheitsniveaus dar [BSI02] und bildet somit zusammen mit den beiden Migrationsstufen (Selbsterklärungen) einen Schritt in Richtung „messbare“ Sicherheit, basierend auf einem etablierten und praxisbewährten Katalog von Standard-Sicherheitsmaßnahmen.

## 3 Auditierung

### 3.1 Regulative Vorgaben

Im Bereich Datenschutz verfolgt das Datenschutzaudit das Ziel, ein Verfahren zu einem messbaren Datenschutz- und Datensicherheitsniveau vorzugeben. Willenserklärungen und Ansätze zu einem Datenschutzaudit finden sich zahlreich, ob in einschlägigen Studien oder bereits in der Gesetzgebung verankert. Allen gemein sind die Prinzipien der Freiwilligkeit und der Transparenz (optionale Veröffentlichung der Ergebnisse). Auch wenn nach Recherche der Autoren einzig der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der GI in seiner Erklärung vom Mai 2000 die Begriffe Datensicherheit und IT-Sicherheit synonym verwendet [GI00], lässt sich ein Trend zur Konvergenz hinreichend belegen. Hinsichtlich der technischen und organisatorischen Schutzmaßnahmen orientiert sich der Gesetzgeber strikt an der üblichen informationstechnischen Terminologie [BMI01], der Begriffswelt der IT-Sicherheit. Wo beispielsweise der Datenschützer vorher von Zugang redend den Zutritt zu Räumen meinte, fasst die BDSG-Novelle vom Mai 2001 diesen Begriff unmissverständlich. Kriterien der schwer abgrenzbaren Datenschutz-Terminologie hinsichtlich „Benutzerkontrolle“ und „Speicherkontrolle“ werden der „Zugriffskontrolle“ zugeschlagen. Die „Datenträgerkontrolle“, „Übermittlungskontrolle“ und „Transportkontrolle“ gehen in der „Weitergabekontrolle“ auf, die sich am Schutzziel der Integrität orientiert; ergänzt um ein weiteres primäres Schutzziel der IT-Sicherheit, dem „Verfügbarkeitsgebot“.

Kritisch hingegen begleiten die Autoren den Weg, den das Datenschutzaudit unter den Leitmotiven Stärkung der Selbstkontrolle und Erhöhung der Transparenz für den Betroffenen nimmt. Die bereits 1997 im Mediendienste-Staatsvertrag [MDSStV97] festgeschriebene Absichtserklärung, dass eine Verfahrensregelung durch ein „besonderes Gesetz“ zum Datenschutzaudit erfolge,<sup>2</sup> wird seitens der Exekutive seither allein gestützt durch die Provet-Studie von Roßnagel [Ro99]. Diese schlägt ein formales Gutachter-Verfahren nach Vorbild der §§ 43 und 44 WPO vor. Dabei ist die Frage

<sup>2</sup> Diese lässt bis heute – zusammen mit gleichlautenden Ausführungen in späteren Gesetzgebungen zum Datenschutz – auf sich warten.

zu stellen, wer sich – nicht zuletzt angesichts aktueller Spargebote seitens der Leitungsebene – einem solchen aufwändigen Verfahren des Datenschutzaudits freiwillig unterwirft. Ein Datenschutzaudit gemäß diesem Vorschlag muss sich daher die Kritik gefallen lassen, hauptsächlich als Kompensation für weggefallene Meldepflichten an die Aufsichtsbehörden, u. a. gemäß § 32 Abs. 1 Ziff. 3<sup>3</sup> [BDSG90], zu dienen.

Eine externe Begutachtung nach stringenten, wenig transparenten Kriterien kontrolliert nahezu ausschließlich den betrieblichen Datenschutzbeauftragten. Im Gegensatz hierzu beobachten die Autoren vielfach den Wunsch, als Zielsetzung eines Datenschutzaudits die Unterstützung des betrieblichen Datenschutzbeauftragten in seinem erweiterten Verantwortungsbereich, insbesondere hinsichtlich IT-lastiger Verfahren wie dem Verfahrensverzeichnis und der Vorabkontrolle, in den Vordergrund zu stellen.

Diese Kritik wird auch von Drews/Kranz [DreKra00] vorgetragen. Sie lehnen das Datenschutzaudit gemäß der Roßnagel-Studie als dritte Kontrollebene zusätzlich zu den etablierten Instrumenten des betrieblichen Datenschutzbeauftragten und den Aufsichtsbehörden ab, da dies „ineffizienten Aufwand und eine deutliche Schwächung der weisungsfreien, unabhängigen Stellung des betrieblichen Datenschutzbeauftragten zur Folge haben würde“. Sie äußern dabei die Meinung, dass sich das Ziel der Realisierung von mehr Datenschutz auch ohne Audit erreichen ließe, durch konsequente Anwendung des bestehenden, dualen Kontrollsystems in Form der betrieblichen Selbstkontrolle und Überprüfungen durch die zuständige Aufsichtsbehörde. Die Zielsetzung zur Schaffung von Wettbewerbsvorteilen erachten sie nur für Teilbereiche (IT-Unternehmen) als sinnvoll und sprechen sich in ihrer Kernthese für ein Datenschutzaudit für Spezialgebiete (IT-Bereich, Tele- und Multimediadienste) und gegen eine generelle Konstituierung des Datenschutzaudits aus. Sie entsprechen damit auch der Meinung der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) [GDD99].

<sup>3</sup> Diese Ziffer betrifft die Datenverarbeitung im Auftrag, die laut Aussagen von Aufsichtsbehörden den größten Anteil der gemäß § 32 [BDSG90] erfüllten Meldepflichten ausmacht.

### 3.2 Praxisgetriebene Ansätze

Getrieben von der Ansicht, dass es „nicht an gut gemeinten Ideen und interessanten theoretischen Debatten, wohl aber an Vollzug und Umsetzung“ mangelt [Bäu01], stellt Bäumler einen ersten Praxistest als „neues Instrument auf dem Gebiet des Datenschutzes“ vor (Ziff. A 1.2 [HDSA-SH]), begünstigt durch die schleswig-holsteinische Landesgesetzgebung zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 [LDSG-SH]. Dieser Ansatz bewertet u. a. die Transparenzaspekte der Verwaltungen gegenüber ihren Bürgern, um so die „Vertrauensbasis Datenschutz“ zu stärken. Neben diesem Ansatz zur Auditierung organisatorischer Aspekte werden Merkmale des Systemdatenschutzes in einem weiteren, ebenfalls beim Unabhängigen Landeszentrum für den Datenschutz (ULD) durchgeführten Verfahren, der Verleihung des „IT-Gütesiegels“ auditiert, was die Entwicklung datenschutzfreundlicher Produkte gezielt fördern soll. Auch das quid!-Projekt [quid!] geht mit der Verleihung eines eigenen Siegels diesen Weg.

Als erfolgreicher Praxisansatz sei hier auch das von Königshofen im Bereich der Deutschen Telekom AG praktizierte Verfahren von Audits sowie Lern- und Umsetzungskontrollen in den fachlich unterstellten Bereichen genannt.

### 4 Konvergenz zu bewährten Standards

Sicher stellen alle diese Ansätze Triebfedern zur Förderung eines modernen, technisch unterstützten Datenschutzes dar, deren Methodik an dieser Stelle auch nicht kritisiert werden soll. Die Autoren stehen diesen Zertifizierungsschemata jedoch insoweit skeptisch gegenüber, als sie neue Prüfverfahren anwenden. Transparenz und Akzeptanz der Methodik und des erreichbaren Siegels werden als zunächst äußerst gering beurteilt. Aufgrund der eingeschränkten Zahl möglicher zu auditierender Organisationen dürften weitere Standards zur Abdeckung fehlender Teilbereiche eingeführt werden, was zu einem schwer zu überschauenden „Wildwuchs“ an Datenschutz- und IT-Gütesiegeln führen dürfte. Diese Befürchtung ist in den einschlägigen Gremien nicht neu. Hierzu sei stellvertretend die Erklärung der Gesellschaft für Informatik (GI) zum

Datenschutzaudit [GI00] vom Mai 2000 (im Rahmen der Kommentierungen zu den sich abzeichnenden Novellierungsaspekten der BDSG-Novelle) angeführt.

### 4.1 Methodik des IT-Grundschutz-Ansatzes

In den „klassischen“ Standards ist der Aspekt Datenschutz zwar nicht offen zu Tage getreten, Bemühungen zu einer Integration gab es jedoch bereits. Seitens des Bundesbeauftragten für den Datenschutz [BfD99] wurde mit dem Entwurf eines Datenschutz-Bausteins zum IT-Grundschutzhandbuch in einem ersten Ansatz bereits die Konvergenz zu einem bewährten Standard der IT-Sicherheit [GSHB] gesucht. Die offensichtlich aufgrund interministerieller Zuständigkeitsdebatten nicht offiziell verabschiedeten Bausteinbeschreibungen, Gefährdungs- und Maßnahmenkataloge zum Datenschutz decken im Wesentlichen die organisatorischen Anforderungen des Datenschutzes ab. In einer Zuordnungstabelle wurden erste Ansätze zur Abbildung der damaligen „zehn Regeln zur Datensicherung“ gemäß Anlage zu § 9 [BDSG90] aufgezeigt, flankiert vom Hessischen Landesbeauftragten für den Datenschutz mit einer Transposition der Anforderungen aus dem Hessischen Landesdatenschutzgesetz.

Die Autoren haben diesen Ansatz Anfang 2003 aufgegriffen. Mit einer praxisorientierten Studie und einem anschließenden Pilotprojekt sollte die postulierte Konvergenz verifiziert werden. Wesentlicher Antrieb zur Auswahl genau dieser Idee war der oben beschriebene Gesichtspunkt der Akzeptanz bewährter Methoden. Erste Recherchen und eine anschließende Analyse offenbarten keine prinzipiellen Schwächen des Verfahrens. Kritikpunkte an dem Vorgehen wurden ebenfalls bis dato nicht geäußert.

Analog zur Abbildungsskizze der „zehn Regeln zur Datensicherung“ gemäß Anlage zu § 9 [BDSG90] ist eine Verknüpfungstabelle zu den aktuellen „acht Geboten“ der Datensicherheit gemäß Anlage zu § 9 [BDSG01] entstanden. Ein weiteres Projektziel war die Integration der Vorgehensweise in eine Werkzeugunterstützung, wie sie im Bereich des Grundschutzes üblich ist. Die Realisierung erfolgte mit Hilfe der IT-Sicherheitsdatenbank SAVE® [SAVE]. Jedes Kontrollziel bzw. Gebot ist in einem analog zum IT-Grundschutzhandbuch erstellten Baustein abgebildet und mit entsprechenden Gefährdungen und Maßnahmen verknüpft.

Im Rahmen eines integrierten und standardisierten Verfahrens sind hierbei die Aspekte des Datenschutzes und der Datenschutz-Organisation sowie die sich aus der Anlage zu Anlage zu § 9 [BDSG01] ergebenden Datensicherheitsaspekte eingeflossen. Die im Entwurf des Grundschutz-Bausteins 3.5 („Datenschutz“) festgelegten organisatorischen Aspekte wurden unter Maßgabe der oben beschrieben, zwischenzeitlichen Tendenzen weiterentwickelt. Für ein Datenschutzaudit sind in diesem Teil knapp 300 Maßnahmenempfehlungen in Form von Prüffragen hinterlegt. Diese stellen analog zur Methodik des IT-Grundschutzhandbuchs transparente Prüfkriterien dar und führen somit zu einer qualifizierten und reproduzierbaren Sicht auf die Datenschutz-Bemühungen der jeweiligen Organisation.

Die Zuordnung der technischen und organisatorischen Schutzmaßnahmen gemäß Anlage zu § 9 [BDSG01] zu den relevanten Grundschutzmaßnahmen wurde in Expertenworkshops erarbeitet. Sie werden bei neuen Grundschutz-Maßnahmen [GSHB] entsprechend erweitert. Die Umsetzung erfolgte durch entsprechende Verknüpfungen der Datensicherheitsgebote zu den relevan-

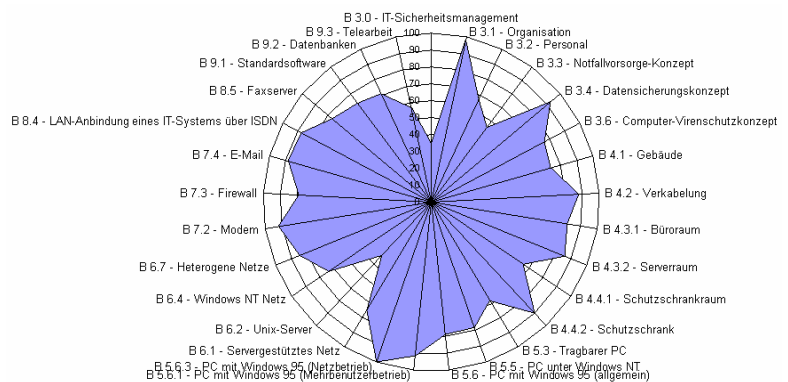


Abb. 1: Ergebnisdarstellung eines Basis-Sicherheitschecks (IT-Grundschutz)

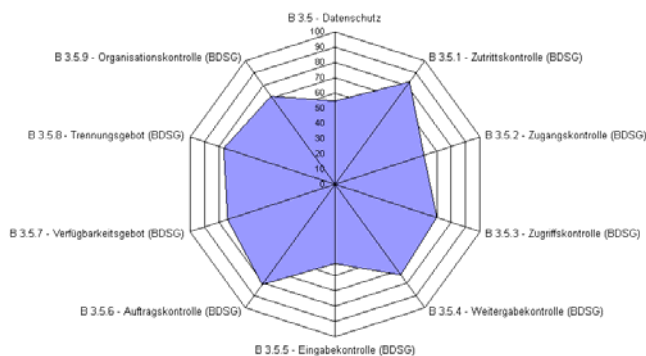


Abb. 2: Ergebnisdarstellung eines Datenschutzaudits (gleicher Datenbestand)

ten Gefährdungen und Grundschutzmaßnahmen. Die insgesamt weit über 1.700 Beziehungen können bei der Durchführung der Überprüfung in Abhängigkeit von der vorhandenen IT-Landschaft, d. h. von den gemäß Modellierungsschema anzuwendenden Bausteinen, ausgewählt werden.

## 4.2 Praxiserfahrungen

Mit der vollständigen Integration der Datensicherheitsbausteine in die bereits angewandte Grundschutz-Vorgehensweise wird nicht nur den geforderten Konvergenzaspekten Rechnung getragen. Es kann zudem eine Verknüpfung bzw. ergänzende Sichtweise auf bereits vorhandene Ergebnisse aus IT-Grundschutzanalysen (siehe Abb. 1) eröffnet werden. Das Vorgehen stärkt somit nachhaltig die effiziente und praxisnahe Anwendbarkeit und die Nutzung bewährter Standards – nicht nur in der Bewertungsweise. Eine Überprüfung der Datenschutz- und Datensicherheitsaspekte (ein Projektbeispiel ist in Abb. 2 dargestellt) eignet sich als Wiederholungsaudit zur IT-Sicherheit und leistet somit seinen Beitrag zur Aufrechterhaltung des Sicherheitsprozesses.

Nach positiven Projekterfahrungen mit der Anwendung in Wirtschaftsunternehmen befindet sich zurzeit die Erstellung eines Moduls für den behördlichen Bereich in Nordrhein-Westfalen in der Realisierungsphase. Dieser Modul unterstützt den behördlichen Datenschutzbeauftragten in der Sicherstellung der technischen und organisatorischen Maßnahmen gemäß § 10 des nordrhein-westfälischen Landesdatenschutzgesetzes [DSG NRW]. Die Pflicht zur Erstellung eines Sicherheitskonzepts gemäß § 10 Abs. 3 [DSG NRW] belegt erneut die Konvergenz zur IT-Sicherheit.

## Fazit

Die Konvergenz von Aspekten des Datenschutzes und der Datensicherheit im BDSG und die vorgestellten Erfahrungen mit einem in der Praxis überprüften, an das Grundschutz-Handbuch angelehnten Prüfungsschema machen deutlich, dass sich IT-Sicherheit und Datenschutz in vielen Aspekten bedingen und ergänzen. Das Synergiepotential einer gemeinsamen Bearbeitung liegt bei der beschriebenen Vorgehensweise auf der Hand. Die Nutzung einer durchgängigen Werkzeugunterstützung, die bereits in der überwiegenden Zahl aktueller IT-Grundschutz-Projekte angewendet wird, macht den Ansatz doppelt wertvoll. Das geschilderte Vorgehen stellt somit nach Meinung der Autoren eine universelle und sinnvolle Praxisumsetzung der noch nicht geregelten gesetzlichen Forderungen nach einem Datenschutzaudit dar. Qualitätsmerkmale unter wirtschaftlichen Aspekten werden ebenso berücksichtigt wie Freiwilligkeit, Selbstkontrolle und Effizienz.

## Literatur

- [Bäu01] Helmut Bäumler, *Datenschutzaudit und IT-Gütesiegel im Praxistest*, RDV 2001, S. 167.
- [BfD99] Entwurf Baustein 3.5 zum IT-Grundschutzhandbuch des BSI, Bundesbeauftragter für den Datenschutz, 1999, [www.bfd.bund.de/technik/DS-KAP/35.htm](http://www.bfd.bund.de/technik/DS-KAP/35.htm).
- [BMI01] Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze, Synopse zu dem am 23. Mai 2001 in Kraft getretenen Änderungen des BDSG.
- [BSI02] BSI (Hrsg.): *Qualifizierung/Zertifizierung nach IT-Grundschutz – Eckpunktepapier*, Stand 25.03.2002, [www.bsi.de/gshb/zert/eckpunkt.htm](http://www.bsi.de/gshb/zert/eckpunkt.htm).

[BDSG90] Bundesdatenschutzgesetz i. d. F. vom 01.06.1991, geändert durch Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990, BGBl. I, S. 2954

[BDSG01] Bundesdatenschutzgesetz i. d. F. vom 23.05.2001, geändert durch Artikel 1 des Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.05.2001, BGBl. I, S. 904.

[DreKra00] Hans-Ludwig Drews, Hans Jürgen Kranz, *Datenschutzaudit*, DuD 4/2000, S. 226.

[DSG NRW] Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen) in der Fassung vom 9. Juni 2000, zuletzt geändert durch Gesetz vom 29. April 2003 (GV. NRW. 2003, S. 252)

[EG95] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der EG vom 23.11.1995 Nr. L 281/31.

[GDD99] GDD-Mitteilungen 2/1999 S. 3

[GI00] Vorschlag des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit“ zu einer Stellungnahme der Gesellschaft für Informatik (GI) zur gesetzlichen Regelung eines Datenschutzaudits, Mai 2000, [www.gi-ev.de/informatik/presse/krypto5.shtml](http://www.gi-ev.de/informatik/presse/krypto5.shtml).

[GSHB] IT-Grundschutzhandbuch, Schriftenreihe zur IT-Sicherheit, Band 3, BSI, Bonn, Bundesanzeiger-Verlag, Stand Mai 2002, aktuelle Version abrufbar unter [www.bsi.de/gshb/deutsch/menuue.htm](http://www.bsi.de/gshb/deutsch/menuue.htm).

[HDSA-SH] Hinweise des ULD zur Durchführung eines Datenschutzbüroaudits nach § 43 Abs. 2 LDSG vom 22. März 2001, Amtsblatt für Schleswig-Holstein, S. 196-200.

[MDStV97] Landesgesetzgebung zum Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag), in Kraft seit 01. August 1997, § 17.

[quid!] Projekt quid!, Qualität im betrieblichen Datenschutz, [www.quid.de](http://www.quid.de)

[Ro99] Prof. Dr. Alexander Roßnagel, *Datenschutzaudit – Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit*, Rechtsgutachten für das BMWA, Projektgruppe verfassungsverträgliche Technikgestaltung (Provet), Universität GH Kassel, Mai 1999, abrufbar u. a. unter [www.iid.de/iukdg/gus/DASA.html](http://www.iid.de/iukdg/gus/DASA.html)

[Ro01] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, *Modernisierung des Datenschutzrechts*, Gutachten im Auftrag des BMI, September 2001

[SAVE] IT-Sicherheitsdatenbank SAVE®, Version 3.0, INFODAS GmbH, 2003, User Manual, Erweiterungsschnittstelle, Kap. 8.2, S. 49, [www.save-infodas.de](http://www.save-infodas.de).