Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)560 H

Betreff: Stellungnahme Bundesdatenschutzauditgesetz zur Anhörung
Von: Karin Schuler <karin@schuler-ds.de>
Datum: Wed, 18 Mar 2009 00:02:10 +0100
An: innenausschuss@bundestag.de

Sehr geehrte Damen und Herren,

als Sachverständige bei der Sitzung des Innenausschusses am 23.3.2009 zur BT-Drs. 16/12011
übersende ich Ihnen anbei eine Vorab-Stellungnahme zur Weiterleitung an die Ausschussmitglieder.
Ich füge außerdem einen Grundsatzartikel zu Datenschutzaudits bei, den ich, gemeinsam mit einem Kollegen, in der Fachzeitschrift "Datenschutz und Datensicherheit" veröffentlicht habe und der einige inhaltliche Erwägungen enthält, deren Fehlen in der Stellungnahme kritisch kommentiert wird.

Mit freundlichen Grüßen,
Karin Schuler

****
Karin Schuler
Datenschutz und IT-Sicherheit

Tel. 0228/24 20 733
karin@schuler-ds.de
http://www.schuler-ds.de

Hammer_Schuler.pdf	**Content-Type:** application/pdf **Content-Encoding:** base64

Stellungnahme_BDSG_Schuler 01.doc	**Content-Type:** application/msword **Content-Encoding:** base64

DVD Deutsche Vereinigung für Datenschutz e. V.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011

1. Allgemeine Bewertung

Die vorgelegten Regelungen eines Datenschutzauditgesetzes sind aus verschiedenen Gründen ungeeignet, das gesteckte Ziel zu erreichen:

- Aufgrund offensichtlich mangelhafter inhaltlicher Auseinandersetzung ist der Auditgegenstand vollkommen unzureichend konzeptioniert.
- Das Verfahren sieht auch für die Inhalte der Richtlinien lediglich die üblichen gesetzlich geforderten Vorgaben vor. Im Ergebnis wird daher lediglich Gesetzestreue, nicht aber ein besonders hohes Datenschutzniveau zertifiziert.
- Das beschriebene, noch nicht einmal einstufige Kontrollverfahren (der Antragsteller soll das Siegel bereits führen, bevor überhaupt auch nur eine einzige Begutachtung stattgefunden hat) kann Datenschutz-Qualität weder fördern noch verlässlich erkennen.
- Die Vermischung kommerzieller Dienstleistung (Kontrollstellen müssen vom Antragsteller bezahlt werden) mit hoheitlichen Aufgaben als Kontrollstelle führt zwingend zu Interessenskonflikten, gefährdet die unparteiische Begutachtung und widerspricht jeglichen international üblichen Zertifizierungsstandards.
- Der vorgesehene bürokratische Aufwand steht in krassem Missverhältnis zu der dünnen und wenig durchdachten Inhalten.
- Das Siegel ist daher ungeeignet, Verbraucherinnen und Verbrauchern verlässliche Entscheidungskriterien zu vermitteln.
- Die alle Fachdiskussionen und praktischen Erfahrungen ignorierende Umsetzung beschädigt das Instrument „Gütesiegel“ mehr als dass sie ihm nutzt. Es würde der Sache eher dienen, auf dieses Gesetz vollständig zu verzichten.

Die vorgelegten Regelungen zur Stärkung betrieblicher Datenschutzbeauftragter sind grundsätzlich zu begrüßen. Sie sind allerdings nicht ausreichend und sollten um Kapazitätsvorgaben ergänzt werden.

Die vorgelegten Regelungen zur Neuordnung des Umgangs mit personenbezogenen Daten zu Zwecken der Werbung, des Adresshandels und der Markt- und Meinungsforschung sind – möglicherweise aufgrund von Lobbytätigkeit der betroffenen Branchen – im Ergebnis so unübersichtlich, dass die Einhaltung kaum erwartet werden kann. Obwohl der Paradigmenwechsel zu einwilligungsabhängiger Datenverwendung zu begrüßen ist, erzeugen die vielfältigen und unübersichtlichen Ausnahmetatbestände einen unakzeptablen Zulässigkeitswirrwarr.

Der vorgelegte Entwurf verwendet außerdem eine Vielzahl von Begriffen aus Informationstechnologie, Zertifizierungsnomenklatur und Datenschutzpraxis in unüblicher, widersprüchlicher oder undefinierter Weise. Dieser handwerkliche und inhaltliche Mangel ist für ein Gesetz unakzeptabel. Auf die diesbezügliche Kritik des Bundesrates wird ausdrücklich verwiesen.

Zu Regelungen des Auditgesetzes

2. Auditgegenstand

Auditierbar sollen laut Gesetzentwurf Datenschutzkonzept oder informationstechnische Einrichtungen sein. Damit ist der mögliche Gegenstand eines Audits jedoch nicht annähernd ausreichend definiert. Was die Schlagworte „Datenschutzkonzept“ und „informationstechnische Einrichtungen“ inhaltlich bedeuten sollen und ob ein Audit alternativ oder gemeinsam beide Gegenstände prüfen soll bleibt unklar.

Eine wesentliche Anforderung an die fachliche Solidität eines Auditgesetzes besteht in der eindeutigen Definition der Prüfgegenstände, so dass die in der Praxis auftretenden Fälle zweifelsfrei und sinnvoll als auditierbar oder nicht auditierbar einzuordnen sind.

Die in der unterschiedlichen Fachliteratur verwendeten Definitionen des Begriffs „Datenschutzkonzept“ zeigen deutlich, dass kein begrifflicher Konsens besteht, auf den ein Gesetz berechtigterweise zurückgreifen könnte.

Die Unterscheidung zwischen „verantwortlichen Stellen“ und „Anbietern von Datenverarbeitungsanlagen und –programmen“ ist in der Praxis unbrauchbar, da es sich nicht um disjunkte Mengen handelt. Die in der Begründung gewählte Unterscheidung zwischen Datenverarbeitungsanlagen und Datenverarbeitungsprogrammen ist in Bezug auf mögliche Auditgegenstände weder fachlich korrekt noch wird auf sie im Weiteren zurückgegriffen. Letztlich wäre nach dieser Pseudo-Definition zwar ein Kabel datenschutzauditierbar (!) nicht aber ein Online-Shop, der auf Standard-Software aufbaut (denn es handelt sich beim Shop-Betreiber nicht um den Anbieter des Programms). Gerade solche Anwendungen sind aber für Verbraucher in Zeiten zunehmender Internet-Geschäfte interessant. Außerdem reicht die Beurteilung des Datenschutzkonzepts allein nicht aus, um den tatsächlichen Datenschutzstandard zu beurteilen. Auf eine Prüfung der Umsetzung, mindestens in geeignet ausgewählten Stichproben, kann seriöserweise nicht verzichtet werden.

Die Einschränkung auf Datenschutzkonzept und informationstechnische Einrichtungen erscheint daher insgesamt deutlich zu kurz gesprungen.

Will man verantwortlichen Stellen die Möglichkeit aussagekräftiger Audits bieten, kommt man um die sachgerechte Definition der Prüfobjekte nicht herum. Dabei muss der fachlich durchdachten Abgrenzung des Prüfgegenstands besondere Aufmerksamkeit gewidmet werden: Wenn nicht das Unternehmen/die Organisation als Ganzes auditiert werden sollen, muss das Prüfobjekt so deutlich für sich stehen, dass keine Gefahr eines pars pro toto-Effekts besteht: dass nämlich das Unternehmen einen kleinen, marginalen Teilbereich prüfen und zertifizieren lässt, anschließend aber in der Öffentlichkeit als insgesamt datenschutzzertifiziert wahrgenommen wird.

3. Datenschutzniveau

Ist bereits die alleinige Einhaltung datenschutzrechtlicher Vorgaben zertifizierungsfähig oder muss ein besonders hohes Datenschutzniveau nachgewiesen werden? Zur Beantwortung dieser Frage wären zwei logische Wege denkbar:

Ist der Gesetzgeber der Meinung, dass eine Mehrzahl der Unternehmen gegen Datenschutzvorschriften verstoßen, müsste eine Zertifizierung verpflichtend eingeführt werden um die Einhaltung der Gesetze zu befördern. In diesem Fall würde lediglich die Gesetzeskonformität bestätigt, was aber keinen Wettbewerbsvorteil brächte.

Geht der Gesetzgeber jedoch grundsätzlich von gesetzestreuer Umsetzung der Datenschutzvorgaben aus, kann ein Zertifikat auf freiwilliger Basis erfolgen. Es bringt jedoch nur dann einen Wettbewerbsvorteil, wenn die gesetzlich vorgeschriebenen Standards deutlich überschritten werden.

Formal wird im vorgelegten Entwurf der Eindruck erweckt, dass in den durch den Auditausschuss erarbeiteten Richtlinien Vorgaben für einen hohen Datenschutzstandard gemacht werden sollen. Die dünnen inhaltlichen Vorgaben führen jedoch lediglich Aspekte auf, die ohnehin Gegenstand gesetzlicher Datenschutzvorgaben sind (§9-Maßnahmen, Einhaltung von Transparenz, Datenvermeidung und Datensparsamkeit).

Im Ergebnis wird daher lediglich Gesetzeskonformität verlangt um ein Zertifikat zu erteilen. Ein Zertifikat dafür, dass jemand keinen Gesetzesverstoß begeht(!) birgt jedoch die falsche Botschaft und ist für Verbraucher wertlos.

4. Kontrollverfahren

Die zur Durchführung der Zertifizierung vorgesehenen Strukturen und Prozesse sind durch übertriebene Bürokratie einerseits und Verletzung grundlegender, international anerkannter Zertifizierungsgepflogenheiten andererseits gekennzeichnet.

Die Möglichkeit zur Führung eines Siegels bevor überhaupt irgendeine Kontrolle des zu zertifizierenden Gegenstands stattgefunden hat, öffnet irreführendem Siegelgebrauch Tür und Tor.

Die fehlende Trennung zwischen begutachtender und zertifizierender Stelle bringt zwingend eine Reihe von Interessenkonflikten mit sich. Die begutachtende Stelle wird vom Auftraggeber bezahlt und ist daher wirtschaftlich nicht unabhängig, wie dies für eine zertifizierende Stelle eigentlich unerlässlich ist. Sie müsste sich nach diesem Gesetzentwurf vielmehr im Falle unzureichenden Datenschutzniveaus gegen den eigenen Auftraggeber wenden, also das Siegel verweigern aber trotzdem eine Rechnung schreiben. Dass hier im Zweifel lieber alle Augen zugedrückt werden, liegt auf der Hand. Die begutachtende Stelle ist außerdem grundsätzlich verpflichtet, jeden Antragsteller zu begutachten, der dies wünscht, unabhängig davon, für wie ausgereift und erfolgversprechend sie dieses Ansinnen hält. Steigt die Zahl der Anträge, muss die begutachtende Stelle aufgrund ihrer regelmäßigen Kontrollpflichten auch für bereits erteilte Siegel die vorhandenen Kapazitäten aufteilen. Es ist nicht davon auszugehen, dass die Kontrollstelle ihre Ressourcen großzügig aufstocken kann. Es ist zu befürchten, dass schon alleine aus Kapazitätsgründen die einzelne

Zertifizierung oder Rezertifizierung einen bestimmten Aufwand nicht überschreiten darf, so dass komplexe Auditgegenstände eher oberflächlich geprüft werden.

Es ist unerklärlich, warum kein Ansatz gewählt wurde, der die Begutachtung durch akkreditierte Sachverständige und die Siegelerteilung durch eine unabhängige Stelle vorsieht, wie dies z.B. in ISO-Verfahren üblich ist. Vor allem die internationale Anerkennung eines Zertifikats ist durch das gewählte Verfahren verunmöglicht.

5. Prüfungsinhalte und Ablauf

Substantiierte Beschreibungen der Prüfungsinhalte fehlen im Gesetzentwurf vollständig. Statt dessen wird diese Aufgabe einem Datenschutzauditausschuss übertragen. Dessen Zusammensetzung lässt jedoch nicht hoffen, dass er die nicht triviale Aufgabe der Festlegung von Prüfungsinhalten für so unterschiedliche Auditgegenstände wie Datenschutzkonzepte und informationstechnische Systeme befriedigend lösen kann.

Es drängt sich der Verdacht auf, dass die Verfasser des vorliegenden Entwurfs mangels ausreichender Kenntnisse den grundlegendsten Teil des Vorhabens delegiert haben um sich dieser unangenehmen Aufgabe zu entledigen. Warum statt dessen ausgerechnet diejenige öffentliche Aufsichtsstelle federführend sein soll, nämlich der Bundesbeauftragte für den Datenschutz, die am wenigsten mit privatrechtlichen Unternehmen und deren Datenschutzorganisation befasst ist, ist unerklärlich. Dies insbesondere deswegen, weil hierdurch eine Parallelkonstruktion zu den eigentlich zuständigen Aufsichtsbehörden aufgebaut wird, die diese schwächt und gleichzeitig die ohnehin zu schwachen Ressourcen durch einen bürokratischen Popanz bindet.

Karin Schuler, stv. Vorsitzende der Deutschen Vereinigung für Datenschutz e.V.
Bonner Talweg 33-35
53113 Bonn
Tel. 0228/24 20 733, Fax. 0228/24 20 734, schuler@datenschutzverein.de

DuD
Datenschutz und Datensicherheit

Cui bono? – Ziele und Inhalte eines Datenschutz-Zertifikats

Volker Hammer, Karin Schuler

Um ein Datenschutz-Zertifikat zur Bestätigung eines hohen Datenschutz-Niveaus erfolgreich zu etablieren, müssen die Randbedingungen stimmen. Ausgehend vom Informationsbedarf möglicher Zielgruppen an ein solches Zertifikat begründet der Beitrag die Datenschutzorganisation als Prüfgegenstand und stellt die aus der Sicht der Autoren wichtigsten Inhalte der Prüfung vor.

Dr.-Ing. Volker Hammer

Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Datenschutz, Anforderungsanalyse, Technikgestaltung, Public Key Infrastrukturen

E-Mail: volker.hammer@secorvo.de

Karin Schuler

Secorvo Security Consulting GmbH. Arbeitsschwerpunkte: Datenschutzorganisation, datenschutzgerechte Technikgestaltung, Privacy Enhancing Technologies

E-Mail: karin.schuler@secorvo.de

Einleitung

„Datenschutzaudit – Quo vadis?“ fragten 2001 einige Autoren in der DuD in einem skeptischen Artikel.[1] Wir möchten in diesem Beitrag einen Blick auf den Nutzen und die Chancen eines Datenschutz-Zertifikats werfen. Obwohl die gesetzgeberischen Aktivitäten zum Datenschutz-Audit seit geraumer Zeit ruhen,[2] wird in der Datenschutz-Szene zunehmend diskutiert, wie dem Datenschutz durch Zertifikate auf die Sprünge zu helfen sei. Als Ergebnis eines erfolgreichen Datenschutz-Audits würde einem Unternehmen ein Zertifikat erteilt werden, das ein bestimmtes (hohes) Datenschutzniveau bescheinigt. Diese Vision hat der ehemalige Landesbeauftragte für den Datenschutz in Schleswig-Holstein, Helmut Bäumler, bereits vor längerer Zeit auf die knackige Aussage „privacy sells“ verkürzt und damit die Überzeugung formuliert, dass Wettbewerbsvorteile durch guten oder gar überdurchschnittlichen Datenschutz diesen insgesamt befördern.

Was aber will man als „hohes Datenschutzniveau“ definieren? Was lässt sich eigentlich in einem Datenschutz-Audit auf welche Weise prüfen? Und was kann ein im Anschluss erteiltes Zertifikat seriöserweise bestätigen?

Fragen, die für die solide Entwicklung eines Datenschutz-Zertifikats notwendig, aber leider nicht hinreichend sind. Denn man darf nicht aus den Augen verlieren, dass außerdem der Nutzen für interessierte Unternehmen deutlich erkennbar sein muss, damit sie die notwendigen finanziellen und personellen Ressourcen bereitstellen. Daher müssen wir zunächst fragen: Wann rechtfertigt der Nutzen eines Datenschutz-Zertifikats die Kosten, die ein Unternehmen für die Vorbereitung und Durchführung eines Audits aufbringen muss?

Wir versuchen in diesem Beitrag, sowohl die Erfolgskriterien als auch den methodischen Audit-Ansatz zu beschreiben. Dabei fließen die Ergebnisse bisheriger Arbeiten und Diskussionen wie auch unsere praktischen Erfahrungen bei der Durchführung von Datenschutz-Audits in Unternehmen ein. Die dargestellten Aspekte gelten unabhängig davon, ob das Datenschutz-Zertifikat über ein gesetzlich geregeltes oder in privatwirtschaftlicher Initiative organisiertes Datenschutz-Audit vergeben wird.

1 Zielgruppen

Wann werden sich Unternehmen einen Wettbewerbsvorteil aufgrund eines Datenschutz-Zertifikats versprechen? Es muss, wie Helmut Bäumler formulierte, „etwas zu gewinnen geben“[3]. Die Unternehmen müssen erwarten können, dass die Adressaten des Zertifikats dieses honorieren und ihre Kaufentscheide oder Beauftragung davon abhängig machen. Als mögliche Adressaten einer durch Zertifikate unterlegten Qualitätsaussage sehen wir im Wesentlichen die folgenden vier Zielgruppen.

1.1. Verbraucher

Dass Verbraucher zunehmend kritisch die Datenschutzpraxis von Verkäufern und Händlern unter die Lupe nehmen, ist bereits seit Jahren bekannt[4] und nicht mehr nur ein Phänomen im Bereich des Online Shoppings[5]. Obwohl Käufer dort besonders intensiv auf den rechtmäßigen Umgang mit ihren personenbezogenen Daten achten: Auch im nicht-virtuellen Geschäftsleben wird mehr und mehr nachgefragt, wie Daten verarbeitet, geschützt und weitergegeben werden. Verbraucherunfreundliche Prakti-

[1] Dieckmann et. al. (2001), S. 549 ff.

[2] Vgl. zur Gesetzgebungsgeschichte des § 9a BDSG und zum Diskussionstand zu seiner weiteren Konkretisierung in Simitis (2006), § 9a, Rdn. 12 ff.

[3] Bäumler (2002), S. 325ff.

[4] Vgl. IBM (1999)

[5] Vgl. Simitis (2006), § 9a Rn. 4f.

ken wie der Adresshandel und andere Zweckentfremdung personenbezogener Daten bringen häufiger als früher öffentliche Diskussionen und negative Publicity. Die jährliche Verleihung der Big Brother Awards[6] erfährt inzwischen hohe Aufmerksamkeit in den Medien. Besonders „hoch in der Publikumsgunst“ stand im letzten Jahr der Preisträger der Versicherungsbranche.

Auch das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz greift aktuelle Probleme des Verbraucherdatenschutzes inzwischen auf, z. B. mit einem Gutachten zu Scoring-Verfahren[7].

Von einem Datenschutz-Zertifikat können Verbraucher profitieren, weil ihnen dadurch die Auswahl von Anbietern mit hohem Datenschutz-Niveau erleichtert wird.

1.2 Auftraggeber für Auftrags-DV

Werden externe Dienstleister mit der Durchführung bestimmter Arbeitsschritte oder Prozesse beauftragt, müssen oft auch personenbezogene Daten verarbeitet werden. Die notwendige Übergabe der Daten an den Dienstleister erfolgt dabei häufig unter dem Sonderkonstrukt der Auftragsdatenverarbeitung gemäß § 11 BDSG. Dieses Modell sieht vor, dass der Auftraggeber verantwortliche Stelle bleibt, die Daten im Sinne des BDSG nicht übermittelt werden und daher die Zulässigkeit einer Übermittlung nicht geprüft werden muss. Allerdings sind an eine derartige Beauftragung strenge Bedingungen hinsichtlich der vertraglichen und tatsächlichen Bindung des Auftragnehmers an die detaillierten Anweisungen des Auftraggebers geknüpft. Außerdem muss sich der Auftraggeber versichern, dass der Auftragnehmer die gesetzlichen Grundanforderungen erfüllt und darüber hinaus seine Datenschutzorganisation angemessen und geeignet ist, die überlassenen personenbezogenen Daten vertrags- und datenschutzgerecht zu verarbeiten.

Auftraggeber für Auftrags-DV würden von einem geeigneten Datenschutz-Zertifikat insofern profitieren, als ihnen die Auswahl von Dienstleistern mit hohem Datenschutz-Niveau erleichtert würde. Sie könnten sich auf die Aussage des Zertifikats verlassen und müssten nicht selbst umfassend prüfen, ob der Auftragnehmer datenschutzgerecht arbeitet und daher im Sinne des BDSG geeignet ist.

1.3 Aufsichtsbehörden

Die Datenschutz-Aufsichtbehörden sollen die Einhaltung datenschutzrechtlicher Bestimmungen kontrollieren. Anlass zur Überprüfung eines bestimmten Unternehmens kann dabei entweder der Prüfplan der Behörde oder ein äußerer Anlass wie die Beschwerde eines Betroffenen sein. Lässt sich der zu prüfende Gegenstand nicht nach Aktenlage klären, wird die Behörde eine Prüfung vor Ort vornehmen. Dabei ist sie, wie jeder Revisor, auf aussagekräftige Dokumentation angewiesen.

Aufsichtsbehörden würden von einem Datenschutz-Zertifikat insofern profitieren, als bei den im Rahmen freiwilliger Selbstkontrolle zertifizierten Unternehmen das Datenschutzniveau deutlich höher sein sollte als im allgemeinen Durchschnitt.[8] Bei zertifizierten Unternehmen kann eine aktuelle und sachdienliche Dokumentation der datenschutzrelevanten Prozesse erwartet werden. Eine Prüfung sollte daher erheblich leichter und schneller vonstatten gehen – ohne dass erst umfangreiche Fragebögen beantwortet oder Dokumentationen erstellt werden müssen.[9] Interne Prozesse zur Behandlung von datenschutzrechtlichen Unregelmäßigkeiten sollten den Überblick über Vorfälle und deren Bearbeitungsstand erleichtern.

1.4 Geschäftspartner

Nicht nur bei der Vergabe von Auftragsdatenverarbeitung haben Unternehmen ein großes Interesse an der ordnungsgemäßen Verarbeitung personenbezogener Daten bei ihren Geschäftspartnern. Auch im Falle von Kooperationen, die die Übermittlung personenbezogener Daten einschließen, will sich die ursprünglich speichernde Stelle der Seriosität bei der Weiterverarbeitung sicher sein. Denn wenn im späteren Verlauf der Bearbeitung eines Kundenauftrags Unregelmäßigkeiten auftreten, fällt dies, ungeachtet der rechtlichen Zuständigkeiten, möglicherweise auf sie selbst zurück.

Jedes Unternehmen, das selbst ein hohes Datenschutzniveau realisiert, hat daher ein Interesse daran, seinen Kunden dieses Niveau auch in der gesamten „Dienstleistungskette“ zu bieten. Das Datenschutz-Zertifikat kann daher ein Auswahlkriterium für Geschäftpartner sein und deren Datenschutz-Niveau in der Dienstleistungskette gegenüber Kunden dokumentieren.

2 Basiseigenschaften eines Datenschutz-Zertifikats

Ein Datenschutz-Zertifikat wird nur dann die gewünschte Wirkung erzielen, wenn es mittelfristig einen relevanten Marktwert erreicht. Es muss „sichtbar“ sein und den Adressaten eine hilfreiche Information bieten. Erfolgreiche Vorbilder in Deutschland sind beispielsweise das Zeichen für Geprüfte Sicherheit (GS-Zeichen[10]), der „Blaue Engel“[11] oder das „Bio“-Siegel[12]. Diese Zertifikate sprechen den Endverbraucher an, weil sie einerseits eine große Verbreitung erreichen und andererseits durch den Verzicht auf Differenzierungen in ihrem jeweiligen Bereich eine einheitliche Botschaft vermitteln.

Wir nehmen an, dass für ein Datenschutz-Zertifikat ähnliche Bedingungen gelten. Es ist dann chancenreich, wenn es eine einfache Botschaft transportiert – nämlich das „hohe Datenschutzniveau“ – und mehr als ein Nischen-Zertifikat wird. Dazu muss ein Datenschutz-Zertifikat nach unserer Auffassung die im Folgenden beschriebenen Basiseigenschaften aufweisen.

2.1 Vergleichbarkeit

Damit erteilte Zertifikate aussagekräftig sind, müssen sie zumindest grundlegend vergleichbar sein. Wenn Firmen mit dem Zertifikat werben, wollen sie zum Ausdruck bringen, dass sie besser sind als ihre Mitbewerber ohne Zertifikat und (mindestens) genauso gut wie die anderen, die ebenfalls den Standard erfüllen.

Diese Vergleichbarkeit soll einerseits für Firmen unterschiedlicher Größen, andererseits aber auch für unterschiedliche Branchen gegeben sein. Könnte man diese Vergleichbarkeit nicht erreichen, müssten unterschiedliche Zertifikate vergeben wer-

[6] www.bigbrotherawards.de
[7] Kamp, Weichert (2005)
[8] Vgl. Simitis (2006), § 9a Rn. 28
[9] Vgl. Dix (2006)
[10] Gesetzlich geregelt über das Geräte- und Produktsicherheitsgesetz. (GPSG 2004)
[11] www.blauer-engel.de
[12] Nach http://www.bio-siegel.de/ waren Ende November 2006 über 34.000 Produkte damit gekennzeichnet. Die Nutzung des Siegels ist durch EU und nationales Recht geregelt und geschützt.

den, beispielsweise nach der Größe („das DS-Zertifikat für mittelständische Unternehmen bis 100 Mitarbeiter“) oder Branche („das DS-Zertifikat für Dienstleistungsrechenzentren“). Beide Differenzierungen sind aufwändig, denn durch sie entstünde erheblicher Aufwand für unterschiedliche Prüfschemata und Auditoren-Spezialisierung. Zudem drohte eine „Zerfaserung“ des Zertifikats, die in der Öffentlichkeit nur schwer nachvollziehbar wäre und das Zertifikat letztlich unattraktiv machte.[13]

2.2 Skalierbarkeit

Bei allem Wunsch nach Vergleichbarkeit ist dennoch einleuchtend, dass die Überprüfung sich an der überwiegenden Art der Verarbeitung personenbezogener Daten („sehr sensibel bis unkritisch“) und an der Größe des Unternehmens („Einmannbetrieb oder Weltkonzern“) orientieren muss. Die Prüfung muss daher berücksichtigen, dass ein Klinikum einen höheren Schutzbedarf als ein Sägewerk aufweist und dass ein europäisches Telekommunikationsunternehmen mehr Organisationsbedarf als der Telefonhändler an der Ecke hat.

Außerdem müssen die Kosten für ein Audit tragbar sein. Ein Audit einer kleinen Organisation muss daher in der Regel mit einem geringeren Gesamtaufwand zu bewältigen sein als in einem Großunternehmen.

2.3 Gegenstand des Audits

Bleibt die Frage, was eigentlich in der Praxis tatsächlich geprüft und zertifiziert werden kann, so dass Vergleichbarkeit und Skalierbarkeit gegeben sind. Ein Produktaudit, das die Zertifizierung einer verkäuflichen Software zum Gegenstand hat [14], scheidet an dieser Stelle aus, weil es den hier angenommenen Informationsbedarf der genannten Zielgruppen nicht befriedigen kann. Es wird hier deshalb nicht betrachtet.

Nähert man sich der Frage mit der klassischen Systematik von Revisoren, so erscheinen grundsätzlich drei wesentliche Klassen von Prüfgegenständen denkbar:

- die Überprüfung von Anwendungen/ Applikationen (z. B. SAP/R3) und deren datenschutzgerechtem Betrieb
- die Überprüfung von hinreichend abgrenzbaren Organisationseinheiten innerhalb des Unternehmens (z. B. der Personalabteilung)
- die Überprüfung der Datenschutzorganisation im gesamten Unternehmen einschließlich der zur Qualitätskontrolle und –verbesserung etablierten Prozesse

Die Auditierung innerhalb der ersten beiden Klassen müsste einen hohen Detaillierungsgrad aufweisen. Sie erfordert – wie auch eine Differenzierung nach Unternehmensgröße oder nach Branchen – eine aufwändige Entwicklung spezifischer Prüfschemata. Insbesondere wenn spezialisierte Prüfkataloge für den Bereich der Anwendungen eine einheitliche Prüftiefe[15] und Vollständigkeit[16] garantieren sollen, ist z. B. eine Prüfung eines gesamten SAP/R3-Systems mit seinen firmenspezifischen Anpassungen anders durchzuführen als die eines Archivierungssystems, eines Lotus Notes Systems, einer Online-Banking-Software oder eines bestimmten Online-Shops.

Auch für die Prüfung einer Abteilung gilt Ähnliches: eine starke Diversifizierungsnotwendigkeit ergäbe sich schon allein für die klassischen Abteilungen, wie Personalabteilung, Finanzbuchhaltung, Einkauf oder Revision. Hinzu kommt, dass in sehr großen Unternehmen die Aufgaben einer Abteilung häufig nochmals auf Unterabteilungen mit mehreren Hierarchieebenen aufgeteilt werden. Die Arbeit einzelner Untergruppen zeichnet sich dabei durch einen hohen Spezialisierungsgrad aus. In kleinen Unternehmen hingegen werden die Aufgaben häufig zusammengefasst und Mitarbeiter übernehmen, teils in Personalunion, mehrere Aufgabenbereiche. Im Datenschutz-Audit wäre deshalb beispielsweise der Organisation von Kontrollfunktionen und der Bewältigung von Interessenskonflikten bei zusammengefassten Zuständigkeiten in kleinen Unternehmen große Aufmerksamkeit zu widmen, während in großen Unternehmen eher die Datenflüsse entlang von Workflows genau untersucht werden sollten.

Soweit nur eine Anwendung, ein Verfahren oder eine Organisationseinheit für die Vergabe eines Zertifikats geprüft werden müsste, sehen wir eine zusätzliche Gefahr in der vereinfachenden „pars pro toto“-Wahrnehmung in der Öffentlichkeit:[17] Dass ein Unternehmen ein Zertifikat für seine Personalabteilung erwirbt, besagt nichts über seinen Umgang mit Kundendaten; dass ein Betrieb einen datenschutzgerechten Online-Shop betreibt, nichts über den Umgang mit Zahlungsverkehrsdaten im Präsenzshop. Verbraucher können kaum unterscheiden, ob ein Zertifikat für das gesamte Unternehmen oder nur für einen Teil vergeben wird.

Eine vergleichbare und damit in der Außendarstellung wirkungsvolle Aussage über den Datenschutzstatus eines Unternehmens kann nur auf einer allgemeineren Ebene getroffen werden: nämlich über die durch ein Unternehmen formulierten Datenschutzziele und die Angemessenheit seiner Datenschutzorganisation.[18] Genau diese müssen aus unserer Sicht Gegenstand des Datenschutz-Audits sein.[19] Dabei umfasst die Datenschutzorganisation alle Maßnahmen und Prozesse, mit denen das Unternehmen seine Datenschutzziele entsprechend dem Schutzbedarf der von ihm verarbeiteten Daten umsetzt. Eine daran orientierte Prüfung untersucht beispielsweise nicht, ob jedes einzelne Datum in einem Prozess rechtmäßig erhoben und verarbeitet wurde, sondern sie bewertet, ob und wie betriebliche Prozesse sicher stellen, dass die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in jedem Fall überprüft und sicher gestaltet wird.

[13] Dies gilt im übrigen auch, wenn Unternehmen jeweils ihren eigenen Datenschutz-Standard definieren könnten (wie dies in Simitis (2006), § 9a Rn. 3f. angenommen wird) und dieser dann durch die Prüfer bestätigt würde.

[14] Vgl. hierzu die Vorgaben und Schemata zum Gütesiegel Schleswig-Holstein

[15] Unter Prüftiefe wird der Detaillierungsgrad und die Nähe zu den „harten Fakten“ verstanden. So geht eine Prüfung der einzelnen Berechtigungen am System tiefer als eine Prüfung der dokumentierten Berechtigungsanträge.

[16] Bezüglich der Vollständigkeit kann unterschieden werden zwischen umfassenden Prüfungen, die alle relevanten Aspekte eines Prüfgegenstandes untersuchen, und Stichproben, die nur ausgewählte Inhalte betrachten.

[17] Die Prüfung von Verfahren schlägt bspw. Rossnagel in seinem Gutachten (Ziffer 3.3) vor. Nach unserem Konzept sollen einzelne Anwendungen oder Geschäftsprozess aber nicht alleine als Gegenstand des Audits gewählt werden können. Sie hätten ihre Stellenwert allerdings im Rahmen der vertiefenden Stichproben, vgl. unten.

[18] Insofern verfolgt unser Vorschlag in einigen Punkten einen ähnlichen Ansatz, wie dies für die Sicherheitsorganisation nach BS 7799 bzw. der Weiterentwicklung nach ISO 27001 der Fall ist (vgl. dazu z.B. Völker 2004 mwN).

[19] § 9a BDSG bezieht das Datenschutz-Audit unter anderem für „datenverarbeitende Stellen [auf] ihr Datenschutzkonzept sowie ihre technischen Einrichtungen“. Darunter könnte auch die Datenschutzorganisation in unserem Verständnis fallen. Die gesetzliche Ausgestaltung steht aber bislang aus.

2.4 Zwischenbilanz

Die Vergabe unterschiedlicher Zertifikate halten wir wegen der Notwendigkeit spezieller Prüfkataloge und vieler unterschiedlich spezialisierter Auditoren nicht für sinnvoll. Sie lassen hohe Kosten erwarten und bieten keine ausreichende Vergleichbarkeit. Damit scheiden größenabhängige und branchenspezifische Zertifikat aus. Die Aussagekraft anwendungs- oder abteilungsbezogener Zertifikate halten wir für relativ begrenzt, so dass damit seriöse Wettbewerbsvorteile kaum erreichbar sein dürften. Außerdem wären für diese vier Varianten nur geringe „Mengeneffekte“ zu erwarten, was wiederum die Wahrnehmung in der Öffentlichkeit und den Nutzen für die Unternehmen begrenzt. Die Marktchancen für differenzierte Zertifikate erscheinen uns deshalb gering.

Als Zwischenbilanz halten wir fest: Zur Feststellung eines hohen Datenschutzniveaus sollte in einem Audit die angemessene, wirksame und rechtskonforme Datenschutzorganisation eines Unternehmens geprüft werden. Ein nach einem erfolgreichen Audit erteiltes Zertifikat bescheinigt, dass eine in betriebliche Prozesse integrierte Datenschutzorganisation als Grundlage für die rechtskonforme Verarbeitung personenbezogener Daten besteht. Es soll für alle geprüften Unternehmen gleich sein und keine Spezialisierungen oder Abstufungen enthalten.

3 Aussagen des Zertifikats

Für die oben vorgestellten Zielgruppen ergeben sich in Bezug auf die Aussagekraft eines Zertifikats durchaus unterschiedliche Erwartungen. Während Verbraucher eher eine allgemeine Aussage über den sorgsamen Umgang mit ihren Daten erwarten, werden potenzielle Auftraggeber für Auftrags-DV auf präzisere Formulierungen zum Umfang der geprüften Fragestellungen Wert legen. Wenn dennoch ein einheitliches Zertifikat vergeben werden soll, müssen für ein zertifiziertes Unternehmen die folgenden Kernaussagen zutreffen:

- Als Verbraucher kann ich davon ausgehen, dass mit meinen Daten nicht nur gesetzeskonform, sondern besonders sorgsam umgegangen wird.
- Datenschutz wird von dem zertifizierten Unternehmen als Grundrechtsschutz und als Qualitätsmerkmal einer verantwortungsvollen Unternehmenstätigkeit verstanden.
- Die Prinzipien Zweckbindung und Erforderlichkeit werden restriktiv interpretiert: Datensparsamkeit und Datenvermeidung werden wirksam umgesetzt.
- Das Datenschutz-Niveau des Unternehmens ist in Bezug auf die Art der verarbeiteten Daten hoch, weil die Datenschutzorganisation gut ist und ständig kontrolliert und verbessert wird. Fehler können erkannt werden und werden unverzüglich beseitigt.

Ein Audit, das die Einhaltung dieser Grundsätze durch Erteilung eines Zertifikats bescheinigt, muss bestimmte Grundlagen immer und einige Gegenstände stichprobenartig prüfen. Wir erläutern im Folgenden unsere Vorstellung von Pflicht und Kür.

4 Audit-Inhalte

Wie also soll die Datenschutzorganisation eines Unternehmens geprüft werden, damit die gewünschten Aussagen getroffen werden können? Die Audit-Inhalte lassen sich nach den folgenden Klassen unterscheiden:[20]

- Pflichtinhalte, die sich aus den gesetzlichen Vorgaben ergeben
- Inhalte, durch die ein hohes Datenschutzniveau nachgewiesen wird.
- Detailprüfung, in denen die Umsetzung der von Maßnahmen stichprobenartig überprüft wird.

Die Inhalte der einzelnen Bereiche werden im Weiteren vorgestellt.

4.1 Gesetzliche Anforderungen

Die Erfüllung gesetzlicher Anforderungen muss eine unabdingbare Voraussetzung für die Erteilung eines Datenschutz-Zertifikats sein. Die Prüfung und Bewertung kann stark formalisiert erfolgen. Es wird geprüft, ob grundlegende Datenschutz-Pflichten sowohl des Unternehmens als auch des Datenschutzbeauftragten erfüllt werden.

Pflichten des Unternehmens

Die Fragen zu den Datenschutz-Grundpflichten eines Unternehmens ergeben sich unmittelbar aus dem Bundesdatenschutzgesetz:

- Besteht eine gesetzliche Pflicht zur **Bestellung eines betrieblichen Datenschutzbeauftragten** und ist das Unternehmen dieser Verpflichtung nachgekommen?
- Ist der betriebliche Datenschutzbeauftragte in der Unternehmenshierarchie korrekt angesiedelt und **direkt der Unternehmensleitung unterstellt**?
- Ist die Zuverlässigkeit des Datenschutzbeauftragten durch **Konfliktfreiheit** mit anderen Aufgaben sicher gestellt und besitzt er die erforderliche Fachkunde?
- Hat der Datenschutzbeauftragte **ausreichenden Zugang zur Unternehmensleitung**? Ist er in betriebliche Prozesse so eingebunden, dass er rechtzeitig Einfluss auf EDV-Anwendungen und –Prozesse nehmen kann?
- Stehen dem Datenschutzbeauftragten ausreichende räumliche, personelle und finanzielle **Ressourcen** zur Verfügung, um seinen Aufgaben angemessen nachzukommen?
- Ist die **Verpflichtung der Beschäftigten** auf das Datengeheimnis nach § 5 BDSG sicher gestellt? Ist gewährleistet, dass die Verpflichteten Art und Umfang ihrer Verpflichtung verstehen?
- Existiert ein vollständiges und aktuelles **Verfahrensverzeichnis** mit den gesetzlich geforderten Angaben? Sind die nach § 9 BDSG Anhang ergriffenen Schutzmaßnahmen systematisch und vollständig dokumentiert? Wird die rechtliche Zulässigkeit der Verfahren geprüft?
- Ist sicher gestellt, dass auf allen denkbaren Übermittlungswegen eintreffende **Auskunftsersuchen Betroffener** sachkundig verarbeitet und beantwortet werden?
- Ist durch betriebliche Prozesse sicher gestellt, dass Verfahren elektronischer Datenverarbeitung rechtzeitig daraufhin untersucht werden, ob sie besondere Gefährdungen für Betroffene mit sich bringen und daher eine formale **Vorabkontrolle** durch den Datenschutzbeauftragten erfordern?
- Sind **Auftragsdatenverarbeitungsverhältnisse** mit Dienstleistern durch datenschutzrechtlich vollständige Verträge ab-

[20] In den folgenden Abschnitten werden auf einer abstrakten Ebene Audit-Inhalte dargestellt, die aus Sicht der Autoren mindestens zu prüfen sind. Ergänzungen sind nicht ausgeschlossen. Die einzelnen Fragen sind für konkrete Prüfkataloge selbstverständlich weiter zu konkretisieren. Dazu kann auf zahlreiche Hinweise aus der Literatur zurückgegriffen werden. Solche finden sich bspw. in Roßnagel (1999b); ULD (2001); Königshofen (1999), S. 266 ff.; Voßbein, DuD 2006.

gesichert? Sofern Auftragsdatenverarbeitung für andere erbracht wird: Ist sicher gestellt, dass der Auftraggeber Herr der Daten bleibt und Verarbeitungen ausschließlich im Rahmen der Beauftragung stattfinden?
- Falls personenbezogene Daten in Staaten außerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie übermittelt werden (**Drittstaaten**): Ist die Zulässigkeit durch Verträge oder Einwilligung hergestellt?

Pflichten des betrieblichen Datenschutzbeauftragten

Die Grundpflichten des betrieblichen Datenschutzbeauftragten ergeben sich ebenfalls aus dem Bundesdatenschutzgesetz. Ihre Erfüllung lässt sich durch folgende Fragen ermitteln:[21]
- Ist durch die innerbetriebliche Organisation sicher gestellt, dass die Beschäftigten regelmäßig in Fragen des **Datenschutzes geschult** werden?
- Hat der Datenschutzbeauftragte einen soliden **Überblick** über die eingesetzten Verfahren?
- **Begleitet und überwacht** der betriebliche Datenschutzbeauftragte planvoll sowohl neue **IT-Projekte** als auch **bestehende Systeme**?
- Wurden alle erforderlichen Anwendungen einer **Vorabkontrolle** unterzogen?

4.2 Fortgeschrittener Datenschutz

Ein Datenschutz-Audit und ein im Anschluss erteiltes Zertifikat haben keinen besonderen Wert, wenn damit lediglich die Einhaltung ohnehin zu erfüllender gesetzlicher Vorgaben bestätigt wird. Dieses Datenschutzniveau müssen alle Unternehmen erfüllen, wollen sie nicht gegen rechtliche Vorgaben verstoßen. Eine Verwertbarkeit für die Außendarstellung setzt voraus, dass der Werbende seine Exzellenz herausstellen und sich damit gegenüber Mitbewerbern hervorheben kann. Ein zertifiziertes Unternehmen muss also mehr tun, als nur im datenschutzrechtlichen Sinne gesetzestreu zu handeln.[22]

Um im Rahmen eines Audits nachweisen zu können, dass das geprüfte Unternehmen mehr als die gesetzlichen Grundforderungen erfüllt, muss es über eine Datenschutzleitlinie mit Mindestvorgaben und eine Datenschutzorganisation verfügen, die diese umsetzt.

Datenschutzleitlinie

Datenschutz kann einem Unternehmen weder ein für allemal verordnet werden, noch bleibt ein bestimmtes Datenschutzniveau nach einer einzigen großen Anstrengung für alle Zeit automatisch erhalten. Um die Daueraufgabe Datenschutz nicht nur von formalen Einflussfaktoren (wie Zeit, Engagement, aktuelles Budget) abhängig zu machen, kommt ihrer Verankerung in den Unternehmensgrundsätzen große Bedeutung zu. Die Erfahrung lehrt, dass ein dauerhaft hohes Datenschutzniveau nur erhalten wird, wenn die Unternehmensführung Datenschutz zu einem wichtigen Prinzip der unternehmerischen Tätigkeit erklärt, schriftlich fixiert und zur verbindlichen Grundlage aller betrieblichen Prozesse und Anwendungen macht. Daher sollte in einem Datenschutz-Audit überprüft werden:
- Existiert eine Leitlinie, in der für das Unternehmen Datenschutz-Mindeststandards verbindlich definiert werden?
- Enthält sie eine Selbstverpflichtung zur kontinuierlichen Verbesserung des Datenschutzniveaus?
- Werden Mindeststandards für das Einholen von Einwilligungen und die Verwendung von Opt-In-Verfahren als Regelfall festgelegt?
- Schließt die Datenschutzleitlinie eine betroffenenfreundliche Informations- und Auskunftspolitik ein?
- Werden alle Fachabteilungen verbindlich zur Zusammenarbeit mit dem Datenschutzbeauftragten verpflichtet? Besteht die Vorgabe, ihn rechtzeitig in Projekte einzubeziehen und ihm umfassend Auskunft zu erteilen?

Die praktische Umsetzung der Vorgaben der Datenschutzleitlinie muss nachgewiesen werden.

Datenschutzorganisation

Wenn ein Unternehmen ein hohes Datenschutzniveau erreichen und kontinuierlich erhalten will, benötigt es eine lernfähige und auf kontinuierliche Verbesserung ausgerichtete Datenschutzorganisation. Dazu muss Datenschutz durchgängig in die Prozesse des Unternehmens integriert sein. In einem Datenschutz-Audit sollten daher mindestens folgende Aspekte geprüft werden:
- Die Aufbauorganisation des Datenschutzes muss geeignet sein, um alle relevanten Unternehmensbereiche abzudecken.
- Das Unternehmen muss über grundlegende Konzepte für die planmäßige, ordnungsgemäße Verarbeitung personenbezogener Daten verfügen und diese wirksam umsetzen. Dazu gehören Dokumentationskonzepte, Berechtigungskonzepte, Löschkonzepte, Konzepte zum Umgang mit Testdaten, Verfahren zu Releasewechseln und weitere.
- Die Sensibilisierung der Beschäftigten muss über das Maß verpflichtender Grundlagenschulungen hinaus gehen (Awarenessmaßnahmen).
- Es müssen Prozesse zur Behandlung von Datenschutzvorfällen etabliert sein, die Verbesserungspotenzial identifizieren und Schwachstellen beseitigen.
- Über eine interne Auditplanung muss sichergestellt werden, dass alle relevanten Unternehmensbereiche in einem sinnvollen Rhythmus überprüft werden. Die dazu notwendigen Prüfpläne und deren Anwendung müssen nachgewiesen werden.

4.3 Vertiefende Stichproben

Die bisher vorgestellten Prüfgegenstände verlangen, dass Strukturen und Abläufe definiert, Verantwortlichkeiten festgelegt, Konzepte erstellt und Maßnahmen dokumentiert werden. Um zusätzlich festzustellen, ob die im Unternehmen definierte Datenschutzorganisation umgesetzt wird und ihre Wirkung entfaltet, muss auch die Datenschutz-Praxis in das Audit einbezogen werden. Dies sollte über vertiefende Stichproben-Prüfungen von Anwendungen und Abteilungen erfolgen.

In vertiefenden Stichproben können verschiedene Prüfgegenstände auditiert werden. Um den Aufwand für die Prüfer und damit auch die Kosten für das geprüfte Unternehmen gering zu halten, sollte dafür im Laufe der Zeit ein Pool von Prüfkatalogen erstellt werden. Der Pool muss hinreichend vielfältige Prüfgegenstände enthalten, um für verschiedene Branchen, Unterneh-

[21] Der Datenschutzbeauftragte muss seine gesetzlichen Pflichten erfüllen. Er kann allerdings nicht für Versäumnisse verantwortlich gemacht werden, die auf mangelnder Unterstützung oder Bereitstellung von Ressourcen durch die Unternehmensleitung beruhen. Bemerkt er Versäumnisse oder Mängel muss er jedoch nachweisbar darauf hinweisen.

[22] Vgl. z. B. Roßnagel (1999b), S. 86; Simitis (2006), § 9a, Rdn. 50 ff.

mensorganisationen und die Arten personenbezogener Daten anwendbar zu sein und dem Prüfer ausreichende Wahlmöglichkeiten zu bieten. Als Prüfgegenstände des Pools bieten sich u. a. an:

- Ist die **Personaldatenverarbeitung** entsprechend der besonderen Sensibilität sicher und datenschutzgerecht organisiert? Bestehen Berechtigungskonzepte für zentrale Personalverwaltungssysteme?
- Sorgt der Datenschutzbeauftragte für eine angemessene Bewertung und Umsetzung von Maßnahmen in **Angelegenheiten des Arbeitnehmerdatenschutzes**?
- Sofern **Videoüberwachung** eingesetzt wird: Wird in öffentlich zugänglichen Bereichen auf die Überwachung hingewiesen? Sind Aufzeichnung, Aufbewahrung, Löschung und Zugriffsrechte datenschutzgerecht organisiert?
- Erfolgt die **Kundenverwaltung** in Übereinstimmung mit dem Prinzip der Datensparsamkeit und den Zwecken, in die gegebenenfalls eingewilligt wurde?
- Werden eventuelle **Scoringverfahren** angekündigt und für die Betroffenen hinreichend transparent gemacht? Wird die Datenbasis so weit wie möglich anonymisiert und pseudonymisiert?
- Als **branchenspezifische Kernabläufe** könnten z. B. die Flüsse von Patientendaten in medizinischen Labors, der Umgang mit Telekommunikations-Verbindungsdaten bei einem Internet-Provider oder der Umgang mit Bestelldaten und Adressen bei einem Online-Shop geprüft werden.
- Im Bereich IT-spezifischer Prozesse und Abläufe wäre die **Verwaltung der Zugangs- und Zugriffsrechte** mit Eintritt, Aufgabenwechsel und Ausscheiden von Mitarbeitern ein sinnvoller Prüfgegenstand.
- Als **Organisationseinheiten** könnten beispielsweise die Personalabteilung, Vertrieb und Marketing, Buchhaltung oder andere geprüft werden. Sinnvoll wäre auch die Überprüfung der Steuerung und Überwachung von Verhältnissen der Auftragsdatenverarbeitung.

Ziel der Stichprobenprüfung ist es nicht, den einzelnen Prüfgegenstand in allen Details zu untersuchen. Der Auditor muss aber überzeugt sein, dass der jeweilige Prüfgegenstand vom Unternehmen datenschutzrechtlich korrekt bewertet und in der Datenschutzorganisation angemessen berücksichtigt wurde. Die hierfür erforderliche Definition von Anforderungen und deren Umsetzung in Richtlinien, Aufgabenverteilung, Arbeitsanweisungen und durch erforderliche Sicherheitsmaßnahmen müssen etabliert sein.

5 Prüfstrategie

Für ein aussagekräftiges Prüfungsergebnis muss durch die Prüfstrategie eine hinreichende Abdeckung aller Tätigkeitsbereiche des Unternehmens erreicht werden. Dies gelingt durch eine geeignete Wahl der Prüfgegenstände. Durch verschiedene Wege der Ergebniserhebung wird gleichzeitig die notwendige Prüftiefe sicher gestellt.

Daher sind für die Prüfung verschiedene Informationsquellen zu verwenden. Da ein hohes Datenschutzniveau untrennbar mit einer guten **Dokumentationspraxis** verbunden ist, können viele der Prüfgegenstände durch eine Begutachtung von Unterlagen bearbeitet werden. Für andere Fragestellungen ist es dagegen sinnvoller, sich durch **Befragungen** und in Workshops vom Stand der Datenschutzorganisation zu überzeugen. Schließlich müssen die **praktischen Prüfungen** von Systemen und Abläufen die Aussagen von Dokumentationen und Interviews bestätigen. Der Auditor muss insbesondere auch bewerten, ob die Dokumentenlage, Interviewaussagen und Workshopergebnisse in sich schlüssig sind und mit den Ergebnissen der praktischen Prüfungen übereinstimmen.

Die Kombination der verschiedenen Erhebungsmethoden ermöglicht den Auditoren an ausgewählten Stellen einen tiefen Einblick in die betriebliche Organisation und damit eine gute Beurteilung des Umsetzungsstandes der Datenschutzmaßnahmen. Die **Auswahl der Prüfgegenstände für Stichproben** sollte daher die Aufgabe des Auditors sein. Um den Eindruck des „Herauspickens von Rosinen“ zu vermeiden, erscheint es sinnvoll, die vertiefenden Stichproben überwiegend aus einem vordefinierten Pool auszuwählen. Ein geringerer Anteil könnte unternehmensspezifisch frei bestimmt werden.. Die Anzahl der Stichproben bestimmt sich durch die Unternehmensgröße, den Umfang der Nutzung personenbezogener Daten und deren Sensitivität.

Die Auswahl der Prüfgegenstände muss eine sinnvolle Kombination aus Prüfungen technischer Systeme, betrieblicher Abläufen und Organisationseinheiten darstellen. Dazu müssen die Besonderheiten des zu prüfenden Unternehmens berücksichtigt werden. In Abhängigkeit von der Organisationsstruktur müssen bekanntermaßen kritische Prüfgegenstände einbezogen werden.

6 Zertifizierungsverfahren

Für die Aussagekraft und Akzeptanz eines Datenschutz-Zertifikats ist es unverzichtbar, dass der Ablauf des Audits und die Vergabe des Zertifikats einem genormten Prozess folgen. Für solche Abläufe gibt es zahlreiche Vorbilder, beispielsweise Ansätze aus der klassischen und EDV-Revision (Revisionsrichtlinien) oder neuere Auditverfahren aus anderen Prüfbereichen, wie z. B. dem Umweltaudit. Das Zertifizierungsverfahren könnte sich auch an erprobten Zertifizierungen aus dem IT-Bereich, wie dem IT-Grundschutz-Zertifikat des BSI, der ISO27001-Zertifizierung oder dem Datenschutz-Gütesiegel Schleswig-Holsteins orientieren. Folgende Grundanforderungen muss das Zertifizierungsverfahren in jedem Fall erfüllen:[23]

- Die Auditoren müssen unabhängig und akkreditiert sein. Sie dürfen dort keine Prüfungen vornehmen, wo sie selbst beratend oder implementierend tätig waren.
- Die Akkreditierungsstellen für Auditoren müssen unabhängig sein.
- Das Zertifikat wird durch eine unabhängige Bestätigungsstelle (Zertifizierungsstelle) vergeben, nachdem sie den Audit-Bericht geprüft hat.
- Zertifizierungsstelle und Akkreditierungsstellen für Auditoren dürfen selbst nicht wirtschaftlich im Bereich der Beratung oder Zertifizierung tätig sein.

Darüber hinaus wäre es sicherlich hilfreich, wenn die Zertifizierungsstelle über internationale Erfahrung und Anerkennung verfügte, um das Gewicht des Datenschutz-Zertifikats auch im Ausland zu garantieren.

Damit ein Unternehmen ein einmal erteiltes Zertifikat für die Außendarstellung weiter verwenden darf, muss es sich in einem bestimmten Turnus, z. B. alle drei Jahre, einer Wiederholungsprüfung (Rezertifizierung) unterziehen. Dabei muss überprüft werden, ob die entscheidenden Datenschutz-Prozesse nach wie vor etabliert sind. Außerdem sollten auch einige vertiefende Stichproben durchgeführt werden. Wenn bei diesen Stichproben auch bisher nicht betrachtete Audit-Gegenstände ausgewählt

[23] Vgl. auch Weichert (2001), S. 268.

werden, wird die Betrachtung des Unternehmens durch Audits im Lauf der Zeit vervollständigt. Der erwartete Aufwand für eine Rezertifizierung sollte aber deutlich geringer ausfallen als der für eine Erstzertifizierung.

Fazit

Wir sind der Überzeugung, dass ein Datenschutz-Zertifikat nur dann die gewünschte öffentliche Wirkung entfalten wird, wenn es an den Fragestellungen von Betroffenen und anderen Zielgruppen orientiert ist, Mengeneffekte erreicht werden und die Aussage bezüglich der verschiedenen zertifizierten Unternehmen vergleichbar ist. Dies könnte mit einem Zertifikat gelingen, das der geprüften Organisation aufgrund einer guten, durchgängigen Datenschutzorganisation und mit Hilfe von Stichprobenprüfungen für einzelne Prüfgegenstände ein hohes Datenschutzniveau bestätigen kann. Durch die sachdienliche Auswahl von Prüfgegenständen kann der Prüfaufwand, abhängig von der Unternehmensgröße und der Sensitivität der verarbeiteten Daten, skaliert werden. Dadurch ist das Konzept für kleine, mittlere und große Unternehmen geeignet.

Die hier dargelegten Argumente gelten aus unserer Sicht gleichermaßen für ein im Sinne des § 9a BDSG rechtlich normiertes[24] wie auch für ein privat etabliertes Datenschutz-Zertifikat. Für beide Varianten müssen inhaltliche Zielsetzung, Marktpotenzial und Vergabeverfahren diskutiert werden, um eine erfolgreiche Einführung sicher zu stellen. Dazu soll dieser Artikel beitragen.

Literatur

Bäumler (2002), Marktwirtschaftlicher Datenschutz, DuD 6/2002, 325 ff.

Dieckmann et. al. (2001), Datenschutz – Quo vadis?, DuD 25/2001, 549 ff.

Dix (2006), Zur Prüfpraxis der Aufsichtsbehörden, DANA 3/2006, 122 ff.

IBM (1999), Multi-National Consumer Privacy Survey, Studie # 938568, Oktober 1999

Kamp; Weichert (2005), Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher, Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, veröffentlicht 2005 unter www.bmelv.de

Königshofen (1999), Prinzipien und Leitlinien für ein Datenschutz-Audit bei Multimediadiensten, DuD 5/1999

Roßnagel (1999), Datenschutzaudit – Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit, provet-Projektbericht.

Roßnagel (1999b), Datenschutzaudit, Vieweg, Wiesbaden, 1999.

Roßnagel, Pfitzmann, Garstka (2001), Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, November 2001

Simitis (2006), Bundesdatenschutzgesetz, 6. Auflage, Nomos, Baden-Baden.

Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein – ULD (2001), Anwendungsbestimmungen des ULD zur Durchführung eines Datenschutzaudits nach § 43 Abs. 2 LDSG, www.datenschutzzentrum.de/material/recht/audit/audit.htm#b4

Völker, (2004): BS 7799 – Von „Best Practice“ zum Standard, DuD 2/2004, 102 ff.

Voßbein (2006): Prüfstandards für den Datenschutz – Hilfe für den Datenschutzbeauftragten, DuD 11/2006, 713 ff.

Weichert (2001), Datenschutz als Verbraucherschutz, DuD 5/2001, 264 ff.

[24] Zahlreiche Argumente für ein Datenschutz-Zertifikat auf rechtlicher Grundlage finden sich in Roßnagel (1999b), 128 ff. und Roßnagel et al (2001), S. 132 ff.