1. Inhaltsverzeichnis

2. Was versteht man unter einem Datenschutz-Audit

EINFÜHRUNG

Ein Datenschutz-Audit bietet einem Unternehmen die Möglichkeit mit der Einhaltung eines überprüfbaren, genormten Mindeststandard zu werben und es dazu zu veranlassen, freiwillig dem Datenschutz einen höheren Stellenwert zu geben, als dies gesetzlich gefordert. Hinzu kommt, daß der vorhandene Standard kontinuierlich verbessert wird.
In der Praxis könnte dies ungefähr so aussehen: Ein Unternehmen überprüft sich selbst auf gewisse, standardisierte Kriterien und erstellt einen Bericht darüber. Dieser Bericht wird von einem unabhängigen Gutachter überprüft und im Erfolgsfall wird das Unternehmen registriert und ihm auf befristete Zeit erlaubt, mit diesem Datenschutz-Audit zu werben. Der Verbraucher könnte sich dann an diesem Audit orientieren und wüßte dann, welche Mindestanforderungen er bezüglich. des Datenschutzes bei diesem Unternehmen erwarten kann. Für das Unternehmen kann die Werbung mit der Erfüllung dieser Anforderungen und die Tatsache, daß dies von einer vertrauenswürdigen Stelle bescheinigt wurde, einen Wettbewerbsvorteil gegenüber anderen Unternehmen, die diese Voraussetzungen nicht erfüllen, bedeuten. Wichtig hierbei ist, daß die Regelung für die Unternehmen freiwillig ist, da ansonsten das Wettbewerbsargument keine Kraft mehr besäße.
Dieses Konzept des Audits wird bereits in anderen Sachgebieten so oder in analoger Form durchgeführt. Als Beispiele seien hier das Umwelt-Audit, geregelt durch die EU-Umweltaudit-Verordnung, und die ISO-Norm 9000 im Bereich der Qualitätssicherung genannt.

ZIELE

Eine Reihe von Zielen könnte mit einem Datenschutz-Audit erreicht werden:
Menschen, die Daten verarbeiten sollen für die Belange des Datenschutzes sensibilisiert werden. Dies ist besonders wichtig, da sich zur Zeit ein sehr großer Teil der Bevölkerung keiner Schuld bewußt ist, wenn sie Daten mißbräuchlich verwendet. Eine ähnliche Wende im Denken, wie sie in den letzten Jahren beim Umweltschutz stattgefunden hat, könnte auch im Bereich des Datenschutzes stattfinden.
Darüber hinaus könnte der Wettbewerb zwischen den Unternehmen stimuliert werden, indem der Verbraucher einen Maßstab dafür in die Hand bekommt, wie mit seinen Daten umgegangen wird.
Beim Datenschutz ist heute in vielen Bereichen kaum gewährleistet, daß die bestehenden gesetzlichen Regelungen auch eingehalten werden, da die Aufsichtbehörden unterbesetzt und überfordert sind. Mit dem Datenschutz-Audit ließe sich die herkömmliche behördliche Kontrolle ergänzen und die

Aufsichtsbehörden könnten entlastet werden und könnten so mehr Ressourcen auf die Kontrolle nicht auditierter Unternehmen verwenden.
Bisher gibt es so gut wie keinen Anreiz für ein Unternehmen, in irgendeiner Form zur Verbesserung des Datenschutzes und der zugehörigen Verfahren und Technologien beizutragen. Im Rahmen des Datenschutz-Audits wäre es möglich, Unternehmen, die eine Vorreiterrolle einnehmen, besonders hervorzuheben. Dies wäre ein großer Wettbewerbsvorteil und somit ein Anreiz zu solch besonderen Anstrengungen.
Im Rahmen des Datenschutz-Audits könnte es möglich sein, das Bewußtsein für den Datenschutz vom betrieblichen Datenschutzbeauftragten auf alle Mitarbeiter zu übertragen, da es um diese Richtlinien zu erfüllen notwendig wird, alle Mitarbeiter in Fragen des Datenschutzes zu schulen.

GESCHICHTE DES DATENSCHUTZ-AUDITS

Der Grundgedanke des Datenschutz-Audits geht auf die EG-Verordnung „über die freiwillige Beteiligung gewerblicher Unternehmen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung“ zurück, welche die rechtliche Grundlage für das sog. Umweltschutz-Audit ist. Letzteres hat wiederum seinen Ursprung in der ISO-Norm 9000 zur Qualitätssicherung.
Die Erwähnung des Datenschutz-Audits im Medienstaatsvertrag (MStV) geht einen Vorschlag der „Projektgruppe verfassungsverträgliche Technikgestaltung“ (provet) zurück. Auch in den ursprünglichen Entwürfen des „Informations- und Kommunikationsdienste-Gesetzes“ (IuKDG) und des „Teledienstegesetz“ war diese Idee verwirklicht. In den verabschiedeten Fassungen fehlten jedoch diese Teile. Der Medienstaatsvertrag regelt in seinem §17 das Datenschutzaudit wie folgt: *„Zur Verbesserung von Datenschutz und Datensicherheit können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“* Ein solches Gesetz ist jedoch bisher noch nicht einmal projektiert, geschweige denn verabschiedet. Mit genaueren Regelungen haben sich inzwischen eine Fülle von Kommissionen, Ausschüssen und Tagungen beschäftigt, z.B. der Sachverständigenrat „Schlanker Staat“, die 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die Enquete-Kommision des deutschen Bundestages „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“, der 62. Deutsche Juristentag u.v.a.m.
Auch in vielen anderen Gesetzentwürfen und dem Landesdatenschutzgesetz von Brandenburg ist ein Datenschutz-Audit vorgesehen. Regeln zur Umsetzung fehlen jedoch auch hier.
Es gibt eine Reihe von Aktivitäten im Bereich der Datenschutz-Prüfungen:
Die Deutsche Telekom AG führt seit 1996 sporadisch interne Datenschutzaudits durch. Die Telekom hat auch den Arbeitskreis „Datenschutzaudit Multimedia“ initiiert. Auch der Arbeitskreis „Datenschutzbeauftragte“ im Verband der Metallindustrie Baden-Württembergs ist der Überzeugung, daß sich seine Mitglieder mit einem Bürokratie-armen und praxisorientiertem Datenschutzaudit anfreunden könnten.
Das Diskursprojekt „quid!“ an der FH Frankfurt a. M. unter Beteiligung der Deutschen Postgewerkschaft sucht nach Möglichkeiten für ein Gütesiegel im Bereich betrieblicher Datenschutz.

VERGLEICH MIT ANDEREN STAATEN

In den Vereinigten Staaten sind mehrere Initiativen entstanden, die zum Ziel haben, die Datenschutzproblematik innerhalb der Industrie selbst zu regulieren und so einem Eingriff des Staates zuvorzukommen. Ein Nebeneffekt dabei wäre es, daß damit auch die Richtlinien anderer Staaten gleich mit erfüllt werden könnten. Dabei werden auch Verfahren entwickelt, die in Richtung eines Datenschutzaudits gehen.
Ein Beispiel hierfür ist die gemeinnützige Initiative „TRUSTe“, deren Mitglieder aus dem Bereich der Online-Industrie stammen. Die Fimen müssen sich verpflichten, die Richtlinien von TRUSTe einzuhalten, ihre Datenschutzpraktiken zu veröffentlichen und die Zustimmung ihrer Kunden zu ihren Praktiken einzuholen. Dann dürfen sie auf Ihrer Homepage ein sog. „trustmark“ anbringen, das den Kunden direkt zur Erklärung der Datenschutzpraktiken führt. Die Einhaltung der Kriterien wird kontrolliert.
In Japan gibt es das dem Datenschutzaudit sehr ähnliche „Japan Information Processing Developement Center“ (JIPDC). Das JIPDC nennt ihr System „Privacy Mark Award System“ und hat einen Katalog von Richtlinien entwickelt. Ein Unternehmen kann an dem System teilnehmen, wenn es über ein adäquates Datenschutzmanagementsystem verfügt. Die Organisation veröffentlicht die zwei Jahre gültige Zertifizierung auf seiner Homepage. Jedes Jahr müssen sich die Betriebe intern auditieren und diese Maßnahmen können dann durch Unabhängige überprüft werden.

3. Anforderungen an ein Datenschutz-Audit

Verschiedene Gruppen der Gesellschaft gehen natürlich mit unterschiedlichen Erwartungen an ein Datenschutzaudit heran:

INTERESSEN DER ANBIETER VON TELEDIENSTEN

Für die Anbieter ist es wichtig, daß ein solches Audit freiwillig ist und daß es Rechtssicherheit bringt. Es muß einen ausreichend hohen Anreiz zur Beschäftigung mit dem Datenschutz geben und das Verhältnis zwischen Kosten und Nutzen muß in einem verträglichen Rahmen liegen. Für kleine und mittlere Unternehmen, die kein eigenes Management für solche Aufgaben haben, sollten Förderungen angeboten werden, die auf diesen Firmen eine Teilnahme am Audit ermöglichen. Wichtig ist, daß die Anforderungen an die Unternehmen weitgehend gleich sind, um Wettbewerbsverzerrungen zu vermeiden. Ebenfalls vermieden werden sollte, daß Konkurrenten aus dem Ausland die mit weniger strengen Richtlinien in einem anderen Land ein Datenschutzaudit bestehen, einen Wettbewerbsvorteil im globalen Markt bekommen. Das Audit soll verläßlich und transparent sein, da es ansonsten keinen wirklichen Vorteil für die Teilnehmer bringt. Die Anforderungen dürfen nicht zu niedrig sein, da ein Audit, das von allen sowieso erfüllt wird a) keine Verbesserungen im Datenschutz bringt und b) nur zu Kosten und Aufwänden führt.

INTERESSEN DER NUTZER

Die Nutzer haben ein Interesse daran, zu wissen, wie ein Unternehmen mit personenbezogenenDaten umgeht. Sie wollen ein Kriterium, mit dem sie verschiedene Anbieter verläßlich beurteilen können, damit sie sich z.B. bei gleichem Preis und gleicher Qualität für den Datenschutz-freundlicheren Anbeiter entschieden können. Es ist wichtig, daß die dargelegten Erkenntnisse glaubwürdig sind, da ansonsten ein Datenschutzaudit seine gesamte Aussagekraft verlieren würde. Die Nutzer wollen, daß Fortschritte im Bereich des Datenschutzes erarbeitet und umgesetzt werden und so neuen Risiken gleich das Wasser abgegraben wird.

INTERESSEN DER ALLGEMEINHEIT

Für die Allgemeinheit ist es wichtig, daß der Datenschutz ständig verbessert wird. Hierzu soll das Datenschutzaudit einen Anreiz geben. Die Schäden durch Datenschutzverletzungen sollen vermindert werden. Bislang machen nur wenige Geschädigte aus Angst vor dem Prozeßrisiko und der Beweislage ihre Ansprüche geltend. Das Audit soll die Aufsichtsbehörden entlasten und ihnen so mehr Zeit für die Kontrolle anderer geben. Es soll darüber hinaus zu einer Sensibilisierung für die Datenschutzproblematik führen.

4. Konzepte

Folgende Aspekte sind bei der Festlegung einer Konzeption erforderlich: Es muß festgelegt werden, wer an dem Verfahren teilnehmen kann, worauf es sich bezieht, nach welchen Kriterien bewertet wird, wie das Audit überprüft werden soll, wie die Unternehmen registriert werden sollen und wie sie das Ergebnis verwenden dürfen sollen, sowie welche Rolle die bereits vorhandenen (betrieblichen) Datenschutzbeauftragten eingebunden werden sollen.

UMWELTSCHUTZ-AUDIT ALS VORBILD

Die bereits erwähnte EG-Verordnung soll nun kurz dargelegt werden.
Durch das Umweltschutz-Audit soll die Verantwortung der Unternehmen für die Umwelt gestärkt werden und Defizite bei der Strafverfolgung gemildert werden. Im Umweltschutzaudit verpflichtet sich ein Unternehmen für einen Standort, die einschlägigen Vorschriften einzuhalten und das Umweltschutzniveau kontinuierlich zu verbessern. Anzustreben ist jeweils die beste wirtschaftlich vertretbare Technik.
Das Verfahren besteht aus neun Abschnitten, die hier nur kurz angeschnitten werden:

a) Das Unternehmen verpflichtet schriftlich sich zu einer bestimmten Umweltschutzpolitik, indem es Ziele und Handlungsgrundsätze festlegt.
b) Das Unternehmen führt selbst eine Umweltprüfung durch, die eine Bestandsaufnahme und eine Sammlung aller relevanter Vorschriften beinhaltet.
c) Auf dieser Grundlage erstellt es einen Katalog mit konkreten Zielen, Maßnahmen und Fristen.
d) Parallel dazu wird ein Umweltmanagementsystem implementiert.
e) Das Unternehmen führt eine Umweltbetriebsprüfung durch, in der analysiert wird, ob Organisation, Management und Betriebsabläufe mit den festgelegten Grundsätzen übereinstimmen. Dies ist spätestens alle drei Jahre zu wiederholen.

f) Als Ergebnis erstellt das Unternehmen eine Umwelterklärung, die veröffentlicht wird und all diese Daten enthält.
g) Ein zugelassener Umweltgutachter überprüft, ob alle Anforderungen der Verordnung eingehalten werden.
h) War die Überprüfung positiv, so wird das Ergebnis bei der IHK bzw. Handelskammer registiert.
i) Jetzt ist das Unternehmen berechtigt, eine festgelegte Teilnahmeerklärung für Werbezwecke zu verwenden.

Die Bundesregierung hat 1998 in ihrem Erfahrungsbericht die Regelung des Umweltschutzaudits „insgesamt als positiv“ bewertet. In Deutschland wurde im Gegensatz zu andern Staaten das staatliche Verfahren dem privaten Verfahren nach ISO 14001 vorgezogen. Da die Erwartungen der Firmen größtenteils erfüllt sind, sind sie auch bereit, den organisatorischen und finanziellen Aufwand zu erbringen. Die Firmen erhoffen sich auch, durch das Umweltschutzaudit das Haftungsrisiko zu minimieren. Es ist wohl zu erwarten, daß sich diese Erkenntnisse auch auf ein Datenschutzaudit übertragen lassen.

MITTEL

Das Wort Audit kommt vom lateinischen «audire» für hören, vernehmen oder im übertragenen Sinne sogar anhören oder vernehmen. Im Bereich der Wirtschaftsprüfung bezeichnet Audit eine Rechnungs- oder Buchprüfung. Im Mittelpunkt steht beim Datenschutzaudit also die immer wiederkehrende interne und externe Überprüfung. Ein Datenschutzaudit sollte natürlich nicht einfach nur überprüfen, ob die gegenwärtigen Gesetze eingehalten werden. Dies würde bedeuten, daß ein Unternehmen dafür prämiert würde, daß es sich rechtskonform verhält! Dies kann wohl nicht im Sinne eines Audits liegen.
Nun stellt sich die Frage, ob das Datenschutzaudit als Systemaudit oder als Produktaudit konzipiert werden soll. Der Unterschied besteht darin, daß beim einem Systemaudit das Unternehmen als ganzes in einem gewissem Bereich untersucht wird, beim Produktaudit jedoch nur ein Produkt auf seine Wirkungen in einem bestimmten Bereich bezogen auditiert wird. Für ein Systemaudit spräche, daß die Firmen als ganzes bewertet würden und auch Datenverarbeitung im übergeordneten Bereich zugrunde gelegt werden. Für ein Produktaudit spräche, daß die Unternehmen mit einem solchen Audit gezielt für ein einzelnes Produkt werben könnten. Ein Problem ist jedoch hierbei, daß ein Datenschutzaudit eigentlich einen dynamischen Prozeß auslösen sollte, der eine kontinuiertliche Verbesserung mit sich bränge. Daher ist ein Datenschutzmanagementsystem vonnöten. Mit den Erfahrungen aus dem oben genannten Umweltschutzaudit sollte wohl anzunehmen sein, daß auch ein Datenschutzaudit als Systemaudit durchgeführt werden sollte.
Ein wesentlicher Faktor ist die Freiwilligkeit. Es kann zwar sein, daß gerade diejenigen Unternehmen mit den größten Defiziten nicht an solchen Auditierungsverfahren teilnehmen; diese könnten dann aber unter marktwirtschaftlichen Druck geraten und schließlich ebenfalls ihren Datenschutz verbessern. Erfolgreich und glaubwürdig wird ein Datenschutzaudit nur dann, wenn nicht alle Unternehmen die Kriterien problemlos erfüllen können, sondern eine gewisse Selektion erfolgt. Entsteht dadurch ein Wettbewerbsdruck auf einzelne Unternehmen, wäre dies genau im Sinne dieses Audits und nicht zu beanstanden.
Der Erfolg des Datenschutzaudits hängt im wesentlichen davon ab, das es eine echte Auszeichnung ist. Nur dann geht ein starker Anreiz von ihm aus. Beim Umweltschutzaudit nehmen nur 2.000 von 300.000 Unternehmen tatsächlich teil. Kritiker werden anmerken, daß eigentlich eine viel höhere Teilnehmer erstrebenswert sei. Dann würde das Audit aber seine Rolle als Auszeichnung verlieren.

ANWENDUNGSBEREICHE

Im folgenden wähle ich für sämtliche Aspekte der Erhebung, Speicherung, Weitergabe und Verarbeitung von Daten den neutralen Begriff Nutzung, um Unterschieden in den Fachsprachen wie z.B. zwischen Juristen und Informationstechnikern entgegenzuwirken.
Eines der größten Probleme beim Datenschutzaudit ist die Frage, was als Gegenstand des Datenschutzaudits gewählt werden sollte. Naheliegend wäre es, das Datenschutzaudit auf die Anwendung der Telekommunikations- und Informationstechnologie zu beziehen. Dabei sollte der gesamte Prozeß, in dem personenbezogene Daten in irgendeiner Form genutzt werden einbezogen werden. Auch für die Aktivitäten anderer Unternehmen, die ein Unternehmen bei der Nutzung seiner Daten unterstützen (z.B. Rechenzentren o.ä.) sollte das letzere Unternehmen in die Verantwortung genommen werden. Eine Erleichterung im Auditierungsprozeß wäre natürlich die Zusammenarbeit mit auditierten Partnern. Aber gerade dieser Ansatz kann, wenn er zu restriktiv gesehen wird, Schwierigkeiten mit sich bringen, insbesondere dann wenn Firmen die Auditierung wegen Zulieferern verweigert würde. Eine Möglichkeit wäre eine Unterscheidung in interne und externe Nutzung von Daten mit unterschiedlichen Ansätzen.

Da das Teledienstgesetz als bisher einziges auf Bundesebene ein Datenschutzaudit vorsieht, sind Teledienste natürlich prädestiniert für ein solches Audit. Teledienste im Sinne des Gesetzes sind Angebote im Bereich des Individualkommunikation, Angebote zur Information und Kommunikation, Angebote zur Nutzung des Internets oder anderer Netze, Angebote zur Nutzung von Telespielen und Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit. Ein Problem ist nicht die Abgrenzung von Diensten im Sinne des Teledienstgesetzes von Diensten im Sinne des Medienstaatsvertrages, sondern die Abgrenzung von Diensten untereinander. Laut Teledienstgesetz gilt z.B. jede Homepage, jede Newsgroup, jeder Shop eines Anbieters als eigener Dienst. Für ein Audit wäre dies wohl wenig zweckmäßig. Geschickter wäre es, diese für den Benutzer in einem Zusammenhang stehenden Dienste gemeinsam zu bewerten, wobei die Ziehung der Grenzen mit Sicherheit nicht einfach ist.
Alle Stellen, die Daten nutzen sollten an Datenschutzaudits teilnehmen können. Grundsätzlich sollten sie auch Behördern offen stehen, mit ein paar Anpassungen in der Ausführung, wie der Ersetzung des externen Gutachters durch eine vorgesetzte Dienststelle. Eine Öffnung des Audits für ausländische Firma könnte es ihnen ermöglichen bei Erfüllung der entsprechenden Kriterien die Akzeptanz bei den inländischen Kunden zu verbessern.

KRITERIEN UND VERFAHREN

Bewertungsgrundlage sollte die Eignung des Datenschutzmanagements für die Anforderungen des Datenschutzes und die Perspektive einer künftigen Verbesserung sein. Als objektiver Maßstab, der sich auf alle Teilnehmer anwenden läßt ist zunächst einmal das Datenschutzgesetz geeignet. Allerdings ist eine Beschränkung auf die Kontrolle der Rechtmäßigkeit nicht adäquat: Niemand sollte dafür belohnt werden, daß er Gesetze einhält – dies sollte selbstverständlich sein! Wichtige Kriterien sind die Information über die Datenerhebung und deren Eigenschaften, eine Technikgestaltung, die es ermöglicht Daten spätestens direkt nach Beendigung der Inanspruchnahme des Dienstes zu löschen und die Daten gegen unbefugte Nutzung zu sichern. Ein weiteres Kriterium ist die Energie, die darauf verwendet wird, so wenig personenbezogen Daten wie möglich zu erheben oder noch besser pseudonyme Verfahren anzubieten. Das gültige Recht sollte ein allgemeinverbindlicher Mindeststandard sein, der notwendig aber bei weitem noch nicht hinreichend sein sollte. Hinzu sollten die Bemühungen kommen, die ein Unternehmen anstrengt, um das Niveau des Datenschutzes kontinuierlich zu verbessern und darüber hinaus eine den Datenschutz berücksichtigende Unternehmenspolitik.
Neben der Tatsache, daß die Grundidee des Datenschutzaudits verwirklicht werden soll, ist noch ein besonderes Problem im Auge zu behalten: Es ist nicht immer einfach, zu gewährleisten, daß an inhaltliche weit differierende Unternehmen ein einheitlicher, vergleichbarer und gerechter Maßstab angelegt wird.
Angelehnt an die Praxis beim Umweltschutzaudit bietet sich folgendes Verfahren an:

1. Die datenverarbeitende Stelle beginnt das Datenschutzaudit damit, daß sie eine Eingangsprüfung durchführt. Diese erbringt für jede Anwendung eine Bestandsaufnahme des Status der Verarbeitung personenbezogener Daten und des Status geltender Datenschutzregeln.
2. Nach dieser Bestandsaufnahmen verpflichtet sich die datenverarbeitende Stelle schriftlich zu einer die gesamte Organisation oder eine Anwendung betreffenden Datenschutzpolitik.
3 Auf dieser Grundlage erstellt die datenverarbeitende Stelle ein Datenschutzprogramm mit den konkreten Datenschutzzielen und dem Katalog konkreter Maßnahmen und dem Fristenplan zur Umsetzung der Datenschutzpolitik für die jeweilige Anwendung.
4. Parallel zum Datenschutzprogramm wird ein Datenschutzmanagementsystem eingerichtet, das die Organisationsstruktur, die Zuständigkeiten sowie die Verfahren, Abläufe und Mittel zur Verwirklichung der Datenschutzpolitik festlegt.
5. In periodischen Abständen führt die datenverarbeitende Stelle selbst eine Datenschutzprüfung als systematische und dokumentierte Analyse durch, ob Organisation, Management und Betriebsabläufe mit der Datenschutzpolitik und dem Datenschutzprogramm übereinstimmen und die angestrebte Verbesserung des Datenschutzes erreicht haben.
6. Als Ergebnis der jeweiligen Betriebsprüfung verfaßt die datenverarbeitende Stelle eine Datenschutzerklärung.
7. Anschließend prüft ein zugelassener unabhängiger Datenschutzgutachter die Datenschutzpolitik, das Datenschutzprogramm, das Datenschutzmanagementsystem, die Datenschutzprüfung und die Datenschutzerklärung und bestätigt die Datenschutzerklärung.
8. Bestätigt der externe Datenschutzgutachter die Datenschutzerklärung wird diese an die zuständige Behörde zur Registrierung im Verzeichnis der am Datenschutzaudit teilnehmenden Stellen weitergeleitet und anschließend veröffentlicht.

9. Aufgrund der Registrierung ist die datenverarbeitende Stelle berechtigt, ein Datenschutzauditzeichen für Werbezwecke zu nutzen.

WERBEWIRKSAMKEIT

Das Datenschutzauditzeichen als Werbemittel ist die eigentliche „Belohnung“ für die teilnehmenden Firmen. Es sagt jedoch nur aus, daß eine Firma das Datenschutzaudit erfolgreich absolviert hat. Zu einer genaueren Beurteilung sollte es noch eine Datenschutzerklärung geben, die darüber Auskunft gibt, aus welchen Gründen das Audit erfolgreich war und wo noch Defizite liegen. Hierzu ist – soweit sich dies bei verschiedensten Unternehmen durchführen läßt – ein möglichst einheitliches Aussehen vonnöten. Folgendes gehört wohl dazu: Der Bericht sollte auch für ein Publikum ohne spezielle Fachkenntnisse verständlich sein. Es sollte transparent alles dargestellt werden, auch mit Zahlen aus vorherigen Prüfperioden, die Rückschlüsse auf die Entwicklung lassen. Und schließlich sollten auch diejenigen Dinge, die noch Probleme bereiten, enthalten sein. Eine solche Erklärung wäre auch beispielsweise für Anleger in Wertpapiere oder Banken ein Maßstab, wie zukunftssicher und kundenorientiert ein Unternehmen ist. Im Bereich des Umweltschutzes gibt es anhand solcher Erklärungen sogar regelrechte Rankings, deren Ergebnisse einen großen Einfluß auf das Image eines Unternehmens haben.
Das Datenschutzzeichen als Werbemittel sollte nicht im Stile eines „blauen Engels“ auf Produkten auftauchen, sondern nur im Zusammenhang mit dem gesamten Unternehmen gesehen werden. Ein Besucher einer Homepage dürfte sicherlich einen positiven Eindruck vom Unternehmen gewinnen, wenn er auf der Titelseite gleich ein solches Zeichen sieht.

ROLLE VON GUTACHTERN UND REGISTRIERUNG

Der in den Unternehmen ohnehin vorhandene Betriebsdatenschutzbeauftragte könnte dabei helfen, Kosten bei der Erstellung des Audits zu minimieren. Er verfügt ohnehin (hoffentlich) über die nötige Fachkenntnis und kann so auch für die Vorarbeiten für das Datenschutzaudit eingesetzt werden. Aufgrund seiner Nähe zum Betrieb weiß er meist auch am besten, wo Verbesserungen möglich und nötig sind und wie diese am besten gestaltet werden.
Die unabhängigen Gutachter spielen eine Schlüsselrolle in dieser Problematik. So müssen in sehr hohem Maße unabhängig und neutral sein, um der Glaubwürdigkeit des Datenschutzaudits nicht zu schaden. Hierbei sind die Erfahrungen im Umweltschutzbereich im Kern übertragbar, d.h. Gutachter müssen eine gewisse, definierte Fachkenntnis nachweisen und integer sein (vergleichbar z.B. mit Wirtschaftsprüfern). Außerdem ist es nötig auch die Gutachter dahingegend zu überwachen, daß sie ihre Aufgaben ordnungsgemäß erfüllen.
Für die Registrierung der Audits muß noch eine passende Stelle gefunden werden. Beim Umweltschutzaudit sind dies die IHKs und Handwerkskammern. Eine andere Möglichkeit, die sich anbieten würde, wäre die Regulierungsbehörde für Telekommunikation und Post, die ohnehin schon Aufsichtsfunktionen hat. Diese Stelle sollte die Ergebnisse des Audits noch einmal auf Plausibilität prüfen und klären, ob der Gutachter auch unbefangen geurteilt hat. Bei Verstößen gegen den Datenschutz können die Einträge auch wieder gelöscht werden.

5. Rechtliche Regelung

Es stellt sich nun die Frage, ob es überhaupt einer gesetzlichen Regelung bedarf. Dies ist zu bejahen, da allein eine solche bewirkt, daß der Verbraucher eine wirkliche Vergleichsmöglichkeit hat. Sonst wäre ein betriebsinternes Audit vielleicht nur ein Werbegag vergleichbar mit den Lebensmittelfirmen, die auf ihren Etiketten anpreisen, daß ihre Produkte „laut Gesetz“ ohne Farb- und Konservierungsstoffe sind. Außerdem führen nicht-vergleichbare Maßstäbe und „Privat-Audits“ zu einer Wettbewerbsverzerrung, die alles andere als im Sinne der Marktwirtschaft ist. Eine Möglichkeit wäre es die Normen des ISO-9000-Reihe auf Datenschutz umzudenken, wobei die Umsetzung der Kriterien auch nicht einheitlich wäre. Außerdem sehen diese Normen keine Punkte wie z.B. kontinuiertliche Verbesserung der Qualität oder Information der Öffentlichkeit vor. Eine rechtliche Grundlage dürfte wohl unentbehrlich sein. Hierzu gehören verbindliche Kriterien und vergleichbare Ergebnisse, eine verbindliche Regelung der Qualifikation und Unabhängigkeit der Gutachter, eine klare Registrierungspolitik und eine Analogie zu bereits genormten Verfahren wie dem Umweltschutzaudit.
Eine rechtliche Regelung kann vom Bund in konkurrierender Gesetzgebung erlassen werden. Aber werden z.B. die IHKs, die von den Ländern beaufsichtigt werden, als Aufsichtsbehörden eingesetzt, so muß der Bundesrat zustimmen.
Ein „Datenauditgesetz“ in Deutschland könnte auch als Vorbild für Europa-weite Regelungen gesehen werden, aber solange es nur in Deutschland gilt und anerkannt wird, könnte es für Unternehmen ein

Hindernis sein, strengere Datenschutzrichtlinien einzuführen, wenn sie den Nutzen nur in Deutschland bekommen. Eine europäische Regelung ist in diesem Zusammenhang sicherlich viel zugkräftiger.
In Zeiten, in denen es üblich ist, über Computernetze weltweit einzukaufen, sollte auch bedacht werden, daß eine weltweite Akzeptanz des Audits den Anreiz wesentlich verbessern könnte. Wer hier gleich abwiegelt, sollte bedenken, daß nicht unbedingt überall ein passendes Gesetz existieren muß. Viele Normen in der Industrie sind sogar „nur“ von Firmen definiert worden und haben sich weltweit durchgesetzt.

6. Fazit

Meiner Meinung nach wäre ein klar geregeltes und kontrolliertes Datenschutzaudit ein wirksames Mittel für den Datenschutz. Es würde der Akzeptanz von e-Business sehr gut tun, wenn man als Verbraucher erkennen könnte, wie mit personenbezogenen Daten umgegangen wird. Der Knackpunkt liegt für mich im System der externen Kontrolle: Mit der Glaubwürdigkeit der gewonnenen Erkenntnisse für den Verbraucher steht und fällt das Datenschutzaudit, da wohl kaum eine Firma Aufwand und Geld in ein Konzept stecken würde, das niemand akzeptiert und das Papier nicht wert ist, auf dem es geschrieben ist. Das viele Firmen solchen Ansätzen skeptisch gegenüber stehen ist verständlich – nicht alle sind bereit Risiken einzugehen. Aber wenn man in unser Informationsgesellschaft ein Mittel zur Hand bekommt, das hilft, einen wichtigen Teil der Privatsphäre des Menschen, seine personenbezogenen Daten, zu bewahren, dann sollte man es mit frischem Mut in die Hand nehmen!

Quellenangaben

Die vorliegende Arbeit besteht im wesentlichen darin, daß ich die mir zur Verfügung stehenden Quellen analysiert und bewertet und schließlich meine eigenen Schlußfolgerungen zusammengefaßt habe.

Quellen:

- Helmut Bäumler (Hrsg.): Der neue Datenschutz: Datenschutz in der Informationsgesellschaft von morgen
- Prof. Dr. Alexander Roßnagel: Datenschutzaudit, Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit (Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie)