KERSTIN BLOSSEY,
BLOSSEY & PARTNER

Datenschutzpraxis: Transparenz für mehr Privatsphäre (Teil 3)

Schwierigkeitsgrad:

„Das Risiko, dass Datenschutzverstöße durch private Unternehmen in die Öffentlichkeit gelangen, ist so hoch wie nie“, leitete der Chief Officer Corporate Data Protection der Daimler AG am 23. April 2009 seinen Vortrag auf einem Fachkongress für internationalen Datenschutz in Berlin ein.

IN DIESEM ARTIKEL ERFAHREN SIE…

Das Prinzip der Selbstkontrolle im betrieblichen Datenschutz;

Meldepflichten gegenüber den Aufsichtsbehörden;

Warum sich der Aufwand für den Datenschutz inzwischen rechnet.

WAS SIE VORHER WISSEN/ KÖNNEN SOLLTEN…

Keine spezifischen Vorkenntnisse erforderlich, die Grundbegriffe des Datenschutzes aus den Artikeln der vorherigen Ausgaben sollten geläufig sein. Alternativ kann auf das Glossar von Blossey & Partner (*http://blossey-partner.de/showpage.php?SiteID=11&lang=1*) zurückgegriffen werden.

Dass er damit einen wunden Punkt ansprechen würde, der ihn höchst persönlich in seiner Funktion als Datenschutzbeauftragter eines weltweit bekannten Konzerns betreffen würde, konnte er, als seine Vortragsunterlagen Wochen vor dem Kongress beim Veranstalter einreichte, noch nicht ahnen. Doch nur wenige Tage vor seinem Vortrag geriet die Daimler AG mit dem Thema des Missbrauchs von Gesundheitsdaten ihrer Beschäftigten selbst als Hauptschlagzeile in den Fokus der globalen Öffentlichkeit. Die Gesellschaft nimmt ihren Anteil an der datenschutzrechtlich vorgesehenen Kontrollfunktion heutzutage also offensichtlich wahr. Doch das Prinzip der Selbstkontrolle geht durch mehrere Instanzen, und gegenüber jeder einzelnen dieser Instanzen ist die Daten verarbeitenden Stelle rechenschaftspflichtig.

In diesem dritten und letzten Teil unserer Serie zum Thema „Transparenz” befassen wir uns mit dem so genannten „internen Verfahrensverzeichnis”, einem sowohl für das Unternehmen als auch für die zuständigen Aufsichtsbehörden grundlegend wichtigen Dokument: Angemessene Transparenz bezüglich der Verfahrensweisen im Umgang mit personenbezogenen Daten ermöglicht die vorgeschriebene Erfüllung von Auskunfts-, Korrektur- und Nutzungs-Widerspruchs-Ansprüchen sowie der Meldepflichten.

Das Grundprinzip der Selbstkontrolle im Überblick

Der betriebliche Datenschutz basiert laut Gesetz auf dem Prinzip der Selbstkontrolle. Dies klingt spontan nach absoluter Freiheit und wenig Verbindlichkeit. Die Kehrseite der Medaille: Nimmt das Unternehmen als Daten verarbeitende Stelle nicht oder nur unzureichend wahr, steigt mit jedem Tag das Risiko eines unzulässigen Umgangs mit teils hoch sensiblen personenbezogenen Daten enorm. Je nach Unternehmensgröße und Komplexität der Geschäftsprozesse wird es mit jedem Tag, der ohne ganzheitliches Datenschutzmanagement gelebt und gewirkt wird, schwieriger und teurer, einen wirklichen Überblick über die tatsächlich gelebten Geschäftsprozesse zu behalten und diese im Sinne der gesetzlichen Anforderungen zu leben. Die Selbstkontrolle ist aber nicht nur Verantwortung der Daten verarbeitenden Stelle, sondern ebenso Verantwortung jedes einzelnen Betroffenen und der Gesellschaft in Summe.

Die Meldepflichten gegenüber den Aufsichtsbehörden aus dem Bundesdatenschutzgesetz (BDSG) heraus sind ein nicht zu vernachlässigender Bestandteil der Selbstregulierung im Datenschutz. Kerngegenstand ist das so genannte „interne Verfahrensverzeichnis”, das von Kollegen und Fachliteratur gelegentlich anders betitelt wird, beispielsweise „Verfahrensregister”. Sehen wir uns – bereits sensibilisiert durch das uneinheitliche Wording – die Schlüsselfakten und die damit verbundene Verdeutlichung der Anforderungen hinsichtlich der zu definierenden, zu analysierenden und schließlich schriftlich zu fixierende Verfahrensaspekte an.

1. Begrifflichkeit und Ausgangssituation

„Verfahren” – Der Begriff meint die Summe aller Geschäftsprozesse, die eine automatisierte Verarbeitung bestimmter personenbezogener Daten zu ein und demselben Geschäftszweck abdecken. Ein Beispiel: ein beliebig sinnvoll zu benennendes Verfahren „Personalkostenabwicklung” kann Lohnbuchhaltung, Gehaltszahlungen, die Meldung an die anhängigen Versicherungs- und Kostenträger sowie alle weiteren Einzelprozesse beinhalten, die im Rahmen dieses Überbegriffs anfallen können. Ein einziges Verfahren kann also mehrere Geschäftsprozesse, rechnergestützte Anwendungen oder Dateien (so genannte „Systeme”) oder auch standardisierte analoge Vorgehensweisen enthalten, was die Erstellung einer Übersicht aller Verfahren in einem zentralen Verzeichnis wesentlich handlicher und aussagekräftiger macht. Im Vordergrund steht bei der Formulierung eines Verfahrens immer der Aspekt des Geschäftszwecks, zu dem die personenbezogenen Daten verarbeitet werden.

„Internes Verfahrensverzeichnis” – Gemäß § 4g Abs. 2 Satz 1 BDSG stellt die verantwortliche personenbezogene Daten verarbeitende Stelle dem Beauftragten für den Datenschutz (DSB) eine Übersicht über die in § 4e Satz 1 BDSG genannten Angaben sowie über die jeweils zugriffsberechtigten Personen zur Verfügung - das so genannte "interne Verfahrensverzeichnis". Der DSB übernimmt an dieser Stelle quasi die Position der Aufsichtsbehörde und erspart in dieser Funktion die gesetzlich vorgesehene Meldung an die offizielle Stelle, die sicherlich wesentlich aufwändiger umzusetzen wäre – allein aus formalen Gründen wie dem äußeren Erscheinungsbild, der maximalen Vollständigkeit der erfassten Verfahren und anderem mehr. Die Datenschutzpraxis hat über die Jahre gezeigt, dass die verantwortlichen Stellen in der Regel nicht über ein Verzeichnis der einzelnen Verfahrensprozesse zur Datenverarbeitung und Verarbeitung personenbezogener Daten verfügten. Etwa 2008 ist hier ein Bewusstsein gewachsen, und die bestellten DSBs haben die Erstellung des entsprechenden Registers in vielen Fällen selbst übernommen, sofern sie dazu qualifiziert und praxiserfahren genug waren. Tatsächlich haben wir bei unseren Kunden in den letzten fünf Jahren kein einziges Unternehmen erlebt, das uns zur Basis unserer Aufgaben das interne Verfahrensverzeichnis hätte zur Verfügung stellen können, so dass der betriebliche DSB sich einer durchaus zeitintensiven Zusatzaufgabe gegenüber stehen sieht.

Alle Verfahren automatisierter Verarbeitung, in denen personenbezogene Daten geschäftsmäßig zum Zweck der (anonymisierten) Übermittlung (§§ 29, 30 BDSG, z. B. Auskunftstätigkeit, Adresshandel, Markt- und Meinungsforschung) verarbeitet werden, sind nach § 4d Abs. 4 BDSG ohne Ausnahme meldepflichtig. Die Meldepflicht für Verfahren, die anderen (Geschäfts-) Zwecken dienen, entfällt, wenn die verantwortliche Stelle einen betrieblichen DSB bestellt hat (§ 4d Abs. 2 BDSG). Bestimmte Stellen sind gemäß § 4f BDSG dagegen generell zur Bestellung eines DSB oder zur Meldung ihrer Verfahren direkt an die Aufsichtsbehörde verpflichtet. Wenn ein fachkundiger zuverlässiger DSB bestellt ist, übernimmt dieser bezüglich des Verfahrensverzeichnisses in vielen Fällen stellvertretend die Kontrollfunktion der zuständigen Aufsichtsbehörde, so dass eine Meldung an die offizielle Dienststelle außerhalb des Unternehmens nicht erforderlich ist, sofern das Unternehmen nicht bestimmten Branchen angehören, die generell den Behörden Auskunft schulden.

Auch wenn keine Pflicht dazu besteht, kann ein DSB bestellt werden, um sich damit von der Meldepflicht zu befreien. Sie entfällt zudem, wenn solche Daten für eigene Zwecke verarbeitet werden, hiermit höchstens neun Personen beschäftigt sind und entweder die Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses (z.B. ein laufendes Bewerbungsverfahren) mit dem Betroffenen dient (§ 4d Abs. 3 BDSG).

2. Erfahrungswerte zum internen Verfahrensverzeichnis

Der Kommentar von Dammann/Simitis zur EG Datenschutzrichtlinie (Art. 18 und 19) gibt bereits eine hinreichend bestimmte Definition für das so genannte Verfahren automatisierter Verarbeitung. Gegenstand eines Verfahrens ist gemäß der EG-Richtlinie, die insoweit durch § 4d BDSG in nationales

deutsches Recht umgesetzt wird, eine „Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen". Entscheidend ist die gemeinsame Zweckbestimmung. Eine Verarbeitung in diesem Sinne kann also durchaus eine Vielzahl von Datenverarbeitungsdateien umfassen. Nach Artikel 18 der Richtlinie unterliegt „eine automatisierte Verarbeitung" personenbezogener Daten oder „eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen" der Meldepflicht. Die Meldepflicht kann sich danach auf jede einzelne automatisierte Verarbeitung eines personenbezogenen Datums beziehen. Anknüpfungspunkt kann aber auch ein so genanntes Bündel von Verarbeitungen sein.

Die Begründung zur EG-Datenschutzrichtlinie bietet für die „Mehrzahl von Verarbeitungen" eine Definition, die für das Verfahren übernommen werden kann. Danach ist ein Verfahren ein Paket der Verarbeitungen, mit denen eine oder mehrere vom Standpunkt des Verantwortlichen der Verarbeitung und der betroffenen Person aus miteinander verbundenen Zweckbestimmungen realisiert werden sollen. Diese Definition geht zunächst von der Zweckbestimmung der Datenverarbeitung aus, wie sie sich nach der Vorstellung des Datenverarbeitenden darstellt.

Zweckbestimmung

Um ein Verfahrensverzeichnis zu erstellen, wäre danach der erste Schritt die Überlegung, für welche Zwecke das Unternehmen Daten verarbeitet. Dabei können mehrere Zwecke in einem Verfahren verbunden sein. So kann beispielsweise ein Datenverarbeitungszweck im Finanzverkehrbereich die „Kontoführung" sein. Im entsprechenden Verfahren zur Kontoführung sind unter anderem alle Soft- und Hardwarekomponenten zu beschreiben - so zum Beispiel verschiedene MS Office-Anwendungen oder eine Software zum Online-Banking, wenn diese Programme für den Zweck „Kontoführung" eingesetzt werden. Daneben gibt es möglicherweise ein Verfahren „Kreditverwaltung" oder ein Verfahren „Immobilienfinanzierung", das dann jeweils entsprechend in der Verfahrensbeschreibung darzustellen ist. Die Daten verarbeitende Stelle kann den Zweck der DV natürlich anders definieren, wenn ihr das praktikabel erscheint. So kann sie etwa die „Kontoführung - Privatkunden" und „Kontoführung - Geschäftskunden" auch als eigenständige Zwecke formulieren, wenn dies zum Beispiel sinnvoll ist, weil diese Teilverarbeitungen mit sehr unterschiedlichen Softwarekomponenten erfolgen. Gegebenenfalls kann neben dem Verfahren „Kreditverwaltung" ein eigenständiges Verfahren „Finanzierungsgeschäfte" formuliert werden, weil diese Verfahren isoliert voneinander betrachtet und übersichtlicher dargestellt werden können. Es hängt von der Organisation in der Daten verarbeitenden Stelle ab, welche Datenverarbeitungszwecke als eine abgeschlossene Einheit betrachtet werden können und zu einem Bündel zusammengefasst sind, das als in sich abgeschlossenes Verfahren betrachtet werden kann.

Es empfiehlt sich nicht, an eine Zweckbestimmung anzuknüpfen, die etwa eine Beschreibung einzelner Word, Excel- oder Accessdateien erfordern würde. Eine zu kleinteilige Verfahrensbeschreibung hat den Nachteil, dass sie nicht mehr überschaubar ist und damit auch nicht den Überblick verschaffen kann, der dem Sinn des Verfahrensverzeichnisses entspricht. Die Zweckbestimmungen sollten außerdem so gewählt und miteinander verbunden werden, dass die von der Datenverarbeitung betroffenen Personen sie nachvollziehen können. Eine Kundin oder ein Kunde wird erkennen können, dass ihre oder seine Daten im Verfahren „Kontoführung" verarbeitet werden. Wohingegen die Personen, die etwa einen Kredit aufgenommen haben, ihre Daten in anderen Verfahren suchen werden. Als Korrektiv für von der verantwortlichen Stelle gewählte Zweckbestimmungen, die ein Verfahren beschreiben, dient also immer die folgende Frage: Lässt sich unter dem gewählten Zweck für die Betroffenen noch erkennen, dass in diesem Verfahren ihre Daten verarbeitet werden? Würde beispielsweise eine Bank ein einziges Verfahren unter dem Gesamtzweck „bankübliche Geschäfte" definieren und alle Datenverarbeitungen der Bank darstellen, wäre dieses Bündel von Datenverarbeitungen zu grob geschnürt. Diese Zweckbestimmung hätte für die von der Datenverarbeitung Betroffenen keine Aussagekraft mehr. Das Einsichtsrecht wäre dann ohne Sinn. Zudem würde diese Bezeichnung nur den allgemeinen Geschäftszweck des Unternehmens beschreiben, nicht aber das oder die Verfahren, die zur Anwendung kommen.

Verantwortliche Stelle

Die Meldepflicht trifft immer die Stelle, die für die Verarbeitung verantwortlich ist. Verantwortlich im Sinne des BDSG sind Stellen nicht nur, wenn sie die Verarbeitung selbst ausführen, sondern auch dann, wenn sie sich hierbei eines Dienstleistungsunternehmens bedienen, das die Verarbeitung in ihrem Auftrag vornimmt (§ 3 Abs. 7 BDSG). Bei einer Auftragsdatenverarbeitung trifft also den Auftraggeber und nicht den ausführenden Auftragnehmer die Meldepflicht. Nach § 4d Abs. 1 BDSG hat die Meldung bereits vor der Inbetriebnahme des meldepflichtigen Verfahrens zu erfolgen. Auch Änderungen der meldepflichtigen Angaben und die Beendigung des meldepflichtigen Verfahrens sind jeweils im Voraus mitzuteilen (§ 4e Satz 2 BDSG). Auf die Frage, wie detailliert die Angaben zu einem Verfahren sein müssen, gab es besondere Auslegungsschwierigkeiten und Diskussionsbedarf bei § 4e Nrn. 4-8 BDSG. Im Zusammenhang zu den Angaben zu einem Verfahren die Nr. 4 BDSG betreffend zur Zweckbestimmung der Datenerhebung, -verarbeitung oder –nutzung müssen demnach gesonderte Angaben zu jedem Verfahren gemacht werden, aus welchen ersichtlich sein muss, welche Zwecke/Ziele konkret damit verfolgt werden.

Granularität der bereitzustellenden Informationen

Formelhafte Angaben, wie zum Beispiel „alle banküblichen Geschäfte", sind für Bürgerinnen und Bürger ohne eigenen Erkenntniswert und daher unzureichend. Nr. 5 BDSG nimmt Bezug auf die Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien. Mit „Daten" sind nicht „personenbezogene Daten" im Sinne des § 3 Abs. 1 BDSG sondern „Datenfeldbezeichnungen" gemeint.

§ 4e Nr. 5 BDSG setzt Art. 19 Abs. 1 der EG-Datenschutzrichtlinie um. Im ursprünglichem Kommissionsvorschlag wurde noch eine „Beschreibung der Art(en) der Daten" verlangt - dieses entsprach dem § 32 Abs. 2 Nr. 6 BDSG. In dem geänderten Kommissionsentwurf wurde daneben die Möglichkeit vorgesehen, sich auf die Angaben von Datenkategorien zu beschränken, damit technische Details, aus denen sich nichts Wesentliches für das Verständnis der betreffenden Verarbeitung ergibt, außen vor gelassen werden können. Mit Daten im Sinne des § 4e Nr. 5 BDSG sind daher „Datenfeldbezeichnungen" gemeint.

Werden Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Jedenfalls soll die Beschreibung der Daten/Datenkategorien stets verdeutlichen, was in Bezug auf die Betroffenen gespeichert wird. Wesentlich ist eine hinreichend detaillierte Darstellung der Datenkategorien. Die verantwortliche Stelle kann gemäß BDSG entweder konkrete Empfänger, an die Daten übermittelt werden, oder lediglich Empfängerkategorien angeben. Wie für Datenkategorien gilt, dass eine abstrahierende Zusammenfassung von bestimmten Empfängergruppen möglich ist. Aber auch hier muss die Bezeichnung hinreichend konkret und für Außenstehende verständlich sein und die Tragweite der Übermittlung erkennen lassen. Eine allgemeine Bezeichnung wie „Kunden" genügt nicht. Mindestens muss erkennbar sein, in welcher Branche oder welchem Betätigungsfeld die Kunden aktiv sind. So könnte eine Empfängerkategorie beispielsweise „Telekommunikationsunternehmen" oder „Versandhandelsunternehmen" lauten.

Regelfristen für die Löschung der Daten

Es genügt hier nicht, sich lediglich auf die „gesetzlichen Aufbewahrungsfristen" zu berufen. Um die geforderte Transparenz für die Bürgerin und den Bürger zu ermöglichen, müssen möglichst konkrete Angaben gemacht werden. Unter Umständen reicht aber die Nennung der einschlägigen Vorschriften aus (etwa in den Fällen des § 35 Abs. 2 Satz 2 Nr. 4 BDSG oder der Hinweis auf eine weitere Speicherung nach HGB-Vorschriften), wenn eine konkretere Antwort nicht möglich ist. § 4e Nr. 8 BDSG fordert die Angabe der geplanten Datenübermittlungen in Drittstaaten (Drittstaaten sind alle Nicht-EU-Länder und Nicht-EWR-Länder). Angaben sind bereits dann zu machen, wenn es mit einer gewissen Wahrscheinlichkeit zu einer Übermittlung kommen wird. Zeitpunkt und nähere Umstände brauchen nicht festzustehen. Bei der Erstanmeldung zum Register sind auch bereits bestehende Übermittlungen zu melden. Hingegen brauchen bei Änderungsmitteilungen wegen neu geplanter Übermittlungen in Drittstaaten bereits bestehende (und gemeldete) Übermittlungen nicht erneut gemeldet zu werden. Eine dahingehende Pauschalisierung, dass die Datenlieferung „in alle Länder der Welt" möglich sei, ist jedoch nicht zulässig. Der Gesetzgeber hat die „Drittstaaten"-Meldepflicht eingeführt, um die Zulässigkeit einer Übermittlung im Einzelfall anhand der datenschutzrechtlichen Bestimmungen des Empfängerlandes beurteilen zu können. Für den Bereich der EU und des EWR geht der Gesetzgeber von einem gleichwertigen Datenschutzniveau aus und verzichtet auf die Meldung. Der pauschale Hinweis auf „alle Länder der Welt" als mögliche Empfänger unterwandert die gesetzgeberische Intention. Es sind konkret die Länder anzugeben, in die Übermittlungen stattfinden oder geplant sind. Von der Meldepflicht zu Nr. 8 sind Fragen der Zulässigkeit der Übermittlung strikt zu trennen. Es kommt nicht darauf an, ob die Übermittlung genehmigungspflichtig ist oder nicht oder ob sie aufgrund von Unternehmensregelungen oder Standardvertragsklauseln erfolgt.

Reduzierte Fassung als öffentliches Verfahrensverzeichnis

Auf Basis vorgenannter Aspekte ist die Erstellung eines internen Verfahrensverzeichnisses als Zusammenstellung der Beschreibungen sämtlicher Verfahren automatisierter Verarbeitungen von personenbezogenen Daten in einem Unternehmen die notwendige und grundlagenbildende Leistung zur Erstellung des Verzeichnisses (Teilregister) zur Einsicht für jedermann oder zur Veröffentlichung, zum Beispiel auf der Unternehmenswebsite; diesen Aspekt haben wir bereits im vorherigen Artikel behandelt.

Wege zum internen Verfahrensverzeichnis

Wie erstellt man nun dieses Dokument, das doch nach einigem Aufwand klingt – und so ist es in der Praxis tatsächlich auch. Dennoch führt kein Weg an dieser etwas komplexen Aufgabe vorbei, das Gesetz ist hier sehr eindeutig. Wie so oft gilt, „viele Wege führen nach Rom", und so liegt es in der Erfahrungsvielfalt, der Kreativität des DSB und des individuellen Unternehmens. Drei Wege, die sich bewährt haben in der Praxis, sind zum Beispiel:

- Musterformulare zum Ausfüllen per Hand (erhältlich z.B. auf den Internetseiten der Aufsichtsbehörden oder diverser Datenschutz-Verlage)
- Software zur automatisierten Erfassung und Aufbereitung der erforderlichen Informationen (Infos z.B. beim Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.)
- Externe Dienstleister, die praxiserfahren sind in Datenschutz, erstellen dieses normalerweise durchaus kostengünstig.
- Eigenentwicklungen, wie z.B. ausfüllbares PDF, das die Bereichverantwortlichen bearbeiten können oder auch eine Datenbank mit einer einfachen graphischen Oberfläche, die sowohl z.B. mit einem Exelfragebogen über das Management als auch vom DSB selbst genutzt werden kann.

Verwendete Quellen:

- Bundesdatenschutzgesetz in der aktuellen Fassung
- Gola, Schomerus: Bundesdatenschutzgesetz Kommentar; 9. Auflage; Verlag C. H. Beck oHG; ISBN: 3406555446;
- Simitis; Bundesdatenschutzgesetz; 6. Auflage; Nomos Verlag; ISBN: 3832913769;
- Berghammer, Möhrle, Herb: Kommentar zum Datenschutzrecht; 37. Lieferung (2008); Boorberg-Verlag; ISBN: 3415006166;

Die aktuellen Datenschutz-Schlagzeilen der Online-Presse im Blick:

Das Redaktionsteam von Blossey & Partner stellt jede Woche neu die Schwerpunktthemen rund um Datenschutz für Sie zusammen unter http://www.blossey-partner.de („News", unten rechts). Das Archiv reicht inzwischen bis 2005 zurück und lässt sich durchsuchen. Viel Spaß beim Stöbern.

In diesem Punkt gilt, dass jedes Unternehmen zusammen mit dem DSB seines Vertrauens gemeinsam die geeignetste Methodik finden muss. Ein für alle gleich gültiges und passendes Produkt gibt es dagegen auf dem Markt nach wie vor nicht.

3. Fazit: transparente Informationspolitik als nutzbringender Mehrwert

Schon seit einigen Jahren predigen wir unseren Kunden geradezu, den Datenschutz, den sie umsetzen und leben, nicht nur als lästige Pflicht, sondern viel mehr als Chance zu betrachten und entsprechend zu kommunizieren. Im Gegensatz zum Qualitätsmanagement-Zertifikat an der Wand gibt es für gelebten Datenschutz sogar eine gesetzliche Anforderung. Unternehmen, die kein Datenschutzmanagement haben, riskieren viel, wie die Presse in den letzten Monaten eindrücklich unter Beweis stellt. Natürlich sind ein paar Millionen Bußgeld für eine Lebensmittelkette aus der Portokasse bezahlbar, strikte Auflagen der Aufsichtsbehörde für den Datenschutzbeauftragten eines Telekommunikationskonzerns lästig und beschämend, aber die Umsatzeinbußen, die das Bekanntwerden der Mängel im Datenschutz an Imageverlust verursacht haben, machen den Millionenbetrag schnell wesentlich schmerzhafter.

Bedenken Sie doch einmal den Umkehrschluss und winken Sie statt nur mit Ihrem Qualitätsmanagement-Urkunde doch einfach mal mit Ihrer umgesetzten Datenschutzorganisation und signalisieren Sie potentiellen wie Bestands-Kunden damit, dass Sie Datenschutz als wichtiges Qualitätsmerkmal verstanden haben und es leben.

Ihre Geschäfts- und Kommunikationspartner werden es Ihnen mit einem Vertrauensvorschuss danken, der immer häufiger sogar über den Zuschlag Ihres Angebots entscheiden kann. Übrigens haben die konkreten Fragen nach dem gelebten Datenschutzmanagement inzwischen auch in Ausschreibungen der öffentlichen Hand Einzug gehalten. Fallen Sie bei der nächsten Angebotserstellung von vornherein aus, weil Sie diese Fragen nicht guten Gewissens beantworten können? Auch Ihr Unternehmen kann mit wenigen Mitteln eine Menge erreichen. Und das nicht nur, was Ihre Informationspolitik betrifft. Lassen Sie sich doch einfach einmal von einem seriösen Datenschutz-Anbieter kostenlos über Ihre Möglichkeiten beraten und machen Sie Nägel mit Köpfen. Ihre Bilanzen werden es Ihnen danken...

„Bußgelder bewegen sich mittlerweile auf einem Niveau, das die Aufmerksamkeit des Managements auf den Datenschutz richtet – insbesondere dann, wenn zusätzlich Schadensersatzklagen in den Raum stehen", höre ich im Vortrag des Daimler-Datenschutzbeauftragten etwas später, und mir ist wieder einmal klar, dass wir, die Endverbraucher und Betroffenen im Sinne des Bundesdatenschutzgesetzes (BDSG) mündig geworden sind.

Für uns als Unternehmer und Entscheider bedeutet das, wir können den Datenschutz in der Tat nicht länger aussitzen oder gar als pro forma-Aufgabe verstehen, sondern müssen ein angemessenes Maß an Aufwand in ein vernünftiges ökonomisch vertretbares Datenschutzmanagement investieren, um schmerzhafte Konsequenzen zu vermeiden. Gut, denke ich mir, dass inzwischen viele meiner innerbetrieblichen und externen Kollegen begriffen haben, dass ein klug durchdachtes Datenschutzkonzept ein überaus wirksames, weil gesetzlich eingefordertes, Qualitätsmerkmal ist, für das man auch mit angemessenem Aufwand ein akzeptables Niveau erreichen kann.

Tipps

- Das interne Verfahrensverzeichnis enthält alle gesetzlich vorgeschriebenen Angaben zum unternehmerischen Umgang mit personenbezogenen Daten und ist von der datenverarbeitenden Stelle dem DSB zur Verfügung zu stellen und von diesem aktuell zu halten.
- Das öffentliche Verfahrensverzeichnis (Verfahrensübersicht) ist eine hervorragende Möglichkeit, datenschutzbewussten Kunden und Interessenten zu signalisieren, dass Sie Datenschutz ernst nehmen und im Unternehmen leben. Nutzen Sie dies, um einen Vertrauensvorschuss zu gewinnen, der sogar über den Zuschlag Ihres Angebots entscheiden kann.
- Haben Sie keinen DSB (z.B. weil dieser gesetzlich für Ihren Betrieb nicht vorgeschrieben ist), müssen Sie die Meldung Ihrer Verfahren in der Regel direkt der zuständigen Aufsichtsbehörde melden.
- Zum Erstellen des internen Verfahrensverzeichnisses gibt es diverse Software, die Sie eventuell nutzen können. Sie sollten diese vor einer Anschaffung zuerst testen. Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat hierzu einige Produkte durch erfahrene DSBs testen lassen und kann Ihnen bei Bedarf evtl. hilfreiche Informationen liefern.
- Eine Software, die Ihnen die Abdeckung sämtlicher Aufgaben des DSB verspricht, sollten Sie mit Vorsicht genießen, denn spätestens beim Kontextbezug werden Sie schnell merken, dass hier ein Computer den Menschen nicht ersetzen kann.
- Wenn Sie sich dafür entscheiden, die bei den Aufsichtsbehörden erhältlichen Formulare zum Ausfüllen zu verwenden, achten Sie auf eine lose Zusammenstellung Ihrer Verfahren, damit Sie bei einer möglicherweise erforderlichen Aktualisierung entsprechende Verfahren mühelos durch aktualisierte Formulare ersetzen können.
- Im Zweifelsfall kann Ihnen die für Sie zuständige Aufsichtsbehörde sicherlich wertvolle Tipps für die praktische Umsetzung geben.

Ausblick aufs nächste Heft:

Im nächsten Heft beschäftigen wir uns mit einem weiteren hochbrisanten Thema aus der Datenschutzpraxis: Whistleblowing. Was ist das eigentlich? Welche Unternehmen müssen das beachten und umsetzen? Wie man kann entsprechende Verfahren datenschutzkonform und unternehmensfreundlich gestalten?

Kerstin Blossey
ist Dipl. Informations-Wirtin (FH) und Gründerin von Blossey & Partner, einem aufstrebenden Unternehmen, das sich ganz auf den betrieblichen/behördlichen Datenschutz spezialisiert hat. Zum Kundenkreis zählen deutsche wie international angesiedelte mittelständische Unternehmen, Konzerne und Einrichtungen aus so unterschiedlichen Branchen wie Telekommunikation, Medien & Presse, Softwareindustrie, Automotive, Wirtschaft, Gesundheitswesen, Tourismus und der öffentlichen Hand.