

Wettbewerbsvorteil durch Datenschutz

von Jürgen Rost

Macht Sie diese Überschrift neugierig? Dann nehmen Sie sich ein paar Minuten Zeit diesen Artikel zu Ende zu lesen, um den Wettbewerbsvorteil, den auch Sie ganz leicht nutzen können, zu erkennen.

Als Begründung zur Entscheidung: Datenschutz „Ja“ oder „Nein“, wird häufig die gesetzliche Pflicht angeführt.

Gut, diese Verpflichtung ist natürlich existent und bietet allenfalls eine Grundlage für weitere, entscheidungsrelevante Gespräche, insbesondere da der Gesetzgeber mit der letzten Änderung des Bundesdatenschutzgesetzes im August 2006 noch einmal klar gestellt hat, dass jedes Unternehmen den Datenschutz zu beachten hat.

Auch wenn die Anzahl der Beschäftigten vielleicht keinen eigens bestellten Datenschutzbeauftragten erforderlich macht, hat doch die verantwortliche Stelle den Schutz der personenbezogenen Daten anderweitig sicher zu stellen (das kann dadurch erfolgen, dass sich der Geschäftsführer selbst fachkundig macht, sich fachkundigen Rat einholt oder freiwillig einen Datenschutzbeauftragten bestellt).

Allerdings finde ich persönlich diese Begründung alleine auf das Gesetz gestützt, ziemlich einfallslos und zudem klingt es wie eine Drohung.

Dabei gibt es doch genügend gute Gründe für den Datenschutz, die noch dazu tatsächlich einen Wettbewerbsvorteil bringen.

Ich möchte Ihnen nun einige gesetzliche Vorschriften aus dem Bundesdatenschutzgesetz vorstellen und dabei direkt den praktischen Nutzen für Ihr Unternehmen aufzeigen:

➤ **Vorschrift 1:**

Unternehmen im nichtöffentlichen Bereich haben ab einer Anzahl von neun Mitarbeitern/innen, die ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, einen Datenschutzbeauftragten zu bestellen.

➤ **Praktischer Nutzen durch den Datenschutzbeauftragten:**

Vertrauen! In Fachkreisen werden Studien vorgestellt, die belegen, dass die Erwartungen bei den Erlösen im Bereich „e-commerce“ bei weitem nicht erfüllt wurden. Als Hauptgrund hierfür wird mangelndes Vertrauen in die neue Technik angegeben. Dieses Misstrauen wird nicht zuletzt durch die vielen Gewinnspiele, Preisausschreiben, Punktesysteme etc. noch zusätzlich gestützt, dienen sie doch nur einem einzigen Zweck, nämlich der Sammlung von Daten über Menschen, deren Gewohnheiten, Kaufkraft etc. Es sollen Profile erstellt werden, die gezielte Werbung ermöglichen. Adressdatenhandel ist, nebenbei bemerkt, ebenfalls ein sehr lukratives Geschäft.

Somit führte dieser Vertrauensverlust eben genau dazu, dass die erwarteten Gewinnprognosen bei weitem nicht erreicht wurden.

Ein Datenschutzbeauftragter, egal ob gesetzlich vorgeschrieben oder freiwillig bestellt, steht für Vertrauen, denn er ist jemand, an den sich jeder wenden kann, der bei Fragen und Problemen für den Kunden „greifbar“ ist. Haben potenzielle Kunden aufgrund eines funktionierenden Datenschutzes mehr Vertrauen in Ihr Unternehmen als in Ihre Konkurrenz, genießen Sie somit schon den ersten Wettbewerbsvorteil!

➤ **Vorschrift 2:**

Die verantwortliche Stelle hat, die mit der Verarbeitung von personenbezogenen Daten beschäftigten Personen, durch geeignete Mittel mit den Vorschriften des Bundesdatenschutzgesetzes vertraut zu machen. Zu Deutsch: die verantwortliche Stelle ist verpflichtet, seine Mitarbeiter/innen zu schulen!

➤ **Praktischer Nutzen durch Schulungen:**

Laut einigen Studien werden die meisten aller Bedrohungsszenarien für betriebsinterne Daten durch die eigenen Mitarbeiter/innen ausgelöst. Davon wiederum ein beachtlicher Großteil durch Unwissenheit und Fahrlässigkeit, nur ein kleiner Rest wird vorsätzlich herbeigeführt.

Schulungen sensibilisieren Ihre Mitarbeiter/innen. Ein(e) geschulte(r) Mitarbeiter/in wird ein nicht zu erratendes Passwort wählen. Wird das Passwort nicht auf einem Zettel unter der Schreibtischauflage „verstecken“ oder – wie so oft – an den Monitor kleben!

Geschulte Mitarbeiter/innen fallen nicht auf die sogenannten „Social-Engineering-Attacken“ herein. Gemeint sind hiermit unter anderem Anrufe von angeblich neuen Mitarbeitern der EDV, die telefonisch das Passwort abfragen möchten.

Geschulte Mitarbeiter/innen speichern keine personenbezogenen Daten auf der lokalen Festplatte, die bei eventuellen Reklamationen von der Festplatte gleich mit an den externen Hardwarespezialisten versandt werden.

Geschulte Mitarbeiter/innen wissen um die Unsicherheit von Emails und verschicken keine Dokumente im Word – Format, da diese meist nur kopiert und Inhalte verändert wurden, allerdings sich der Originaltext leicht wieder herstellen lässt.

Es würde jetzt den Rahmen sprengen, alle Vorteile aufzuzeigen, die geschulte Mitarbeiter/innen gegenüber einem ungeschulten haben. Somit können Sie den größten Unsicherheitsfaktor, so gut es geht, minimieren. Das schaffen Sie nur durch Schulungen und Sensibilisierung Ihrer Mitarbeiter. Denn sind die personenbezogenen Daten Ihrer Mitarbeiter/innen, Kunden und Lieferanten geschützt, dann sind es Ihre unternehmensrelevanten Daten, Ihr Know-How ebenso!

Der Wettbewerbsvorteil liegt also darin, dass Ihre Mitbewerber, die keine Schulungen und keine Sensibilisierung für deren Mitarbeiter/innen praktizieren, ein ungleich höheres Schadensrisiko tragen als Sie!

➤ **Vorschrift 3:**

Die viel diskutierte Verfahrensbeschreibung: Neben dem vom Gesetzgeber geforderten Verzeichnis, welches von der verantwortlichen Stelle zu führen ist und jedermann auf Verlangen in geeigneter Form zugänglich gemacht werden muss, gibt es noch die Verfahrensbeschreibung, die dem Datenschutzbeauftragten von der verantwortlichen Stelle unaufgefordert zur Verfügung gestellt werden muss

➤ **Praktischer Nutzen aus dieser Verfahrensbeschreibung:**

Zugegeben, die Erstellung der Verfahrensbeschreibung ist keine leichte Aufgabe und in der Praxis muss nicht selten der Datenschutzbeauftragte um Unterstützung gebeten werden. Der Zeitaufwand ist ebenfalls nicht unerheblich und doch, die Vorteile überwiegen klar: Durch gewissenhafte und vollständige Verfahrensbeschreibungen werden Geschäftsprozesse transparent. Das Gesamtkonzept wird durchleuchtet und beispielsweise doppelte Datenhaltung, mangelnde Datensicherung oder ein fehlendes Rollen - Rechte Konzept aufgedeckt.

Verfahrensbeschreibungen sind die ideale Anleitung für Ihre Mitarbeiter/innen, von wem, wo, welche personenbezogenen Daten zu welchem Zweck gespeichert, verarbeitet, übermittelt und gelöscht werden dürfen.

Nun haben Sie erfahren, dass eine Verfahrensbeschreibung Ihre Geschäftsprozesse (natürlich nur intern) transparent erscheinen lässt. Das spiegelt ja auch den Grundgedanken des Datenschutzgesetzes wieder und begründet sich in dem Grundrecht auf informationelle Selbstbestimmung. Wenn wir uns nun überlegen, wir haben ein Konstrukt erstellt, einen Rahmen definiert, den wir, gefüllt mit den Angaben über personenbezogenen Daten, die Verfahrensbeschreibung nennen. Wenn wir nun aber dieses Konstrukt, diesen Rahmen mit anderen Daten „füttern“ beispielsweise aus der Fertigung, oder Lagerhaltung etc. dann wird die Ähnlichkeit zu einem Qualitätsmanagement-Konzept sofort klar. Dieses System kann man mit verschiedenen Daten und aus verschiedenen Ansätzen heraus füllen und erreicht diese Transparenz somit in jedem beliebigen Bereich!

Es hilft den Verwaltungsaufwand für alle Bereiche so gering wie möglich zu halten und hier liegt der größte Wettbewerbsvorteil gegen über Ihren Mitbewerbern!

➤ **Vorschrift 4:**

Die technischen und organisatorischen Maßnahmen nach § 9 BDSG werden in der Anlage dazu genauer beschrieben:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Die verantwortliche Stelle ist laut Gesetz dazu verpflichtet, die aufgeführten Punkte im verhältnismäßigen Aufwand durch geeignete Maßnahmen einzuhalten.

➤ **Praktischer Nutzen aus der Einhaltung des Gesetzes:**

Das Bundesdatenschutzgesetz wurde verabschiedet, um Menschen vor Missbrauch im Umgang mit ihren Daten zu schützen. Alle angeführten Kontrollen beziehen sich laut BDSG natürlich in erster Linie auf eben diese personenbezogenen Daten, doch eine Zutrittskontrolle zu Ihrem Firmengelände oder den Serverraum schützt automatisch auch andere Daten, wichtige unternehmensrelevante Daten, Ihr Know-How, das womit sie tagtäglich Ihr Geld verdienen. Eine funktionierende und aktuelle Firewall schützt automatisch all Ihre Daten! Egal um welche Kategorie von Daten es sich handelt!

Wenn die datenschutzrechtlichen Regeln für die Verfügbarkeit von personenbezogenen Daten eingehalten werden, sind automatisch auch alle anderen Daten mittels Backup-Verfahren ständig verfügbar, selbst wenn ein Großfeuer Ihr Rechenzentrum zerstören würde! Letzteres ist für fast alle Unternehmen überlebenswichtig!

Ich habe Ihnen jetzt nur einen Teil der gesetzlichen Vorschriften aufgezeigt und den jeweiligen direkten Nutzen für Ihr Unternehmen aufgezeigt. Fassen wir kurz zusammen:

- ⇒ Der Datenschutz gibt konkrete Vorgaben zum Schutz der personenbezogenen Daten.
Diese Vorgaben und die durch den Datenschutz zum Einsatz kommenden Maßnahmen schützen aber automatisch auch all Ihre anderen Daten!
- ⇒ Die meisten Verstöße und Fehler resultieren aus nicht geschulten Mitarbeitern. Der Datenschutz schreibt Schulungen zwingend vor, somit minimieren Sie Ihr Risiko durch sensibilisierte, aufmerksame und geschulte Mitarbeiter/innen.
- ⇒ Sämtliche, im Datenschutz zum Einsatz kommenden Werkzeuge, lassen sich problemlos auch auf andere Geschäftsbereiche anwenden, somit hilft

⇒ Das wichtigste für Ihr Unternehmen sind Ihre Kunden, Kunden gewinnt man durch Vertrauen, Datenschutz schafft Vertrauen, somit gewinnt der Datenschutz für Sie Kunden.

Jürgen Rost
Thansüß, Zum Steig 3
92271 Freihung

Telefon: 0151-166 795 54
E-mail: info@datenschutzloesungen.de
Internet: www.datenschutzloesungen.de