Betrieblicher Datenschutz

Ralf Wondratschek
28.01.2010

Quellenverzeichnis

1. Einleitung

In der heutigen Zeit kann man nicht mehr davon sprechen, dass es hin und wieder kleinere Datenpannen gibt. Nein, viel eher kann man sagen, dass die Medien regelmäßig von Datenskandalen erschüttert werden. Vorfälle, wie bei Daimler, Lidl oder der Bahn, sind trotz eines fülligen Bundesdatenschutzgesetzes nicht zu verhindern gewesen. Es ist selbstverständlich, dass Fragen zur Bekämpfung solcher Skandale aufkommen. Einige Personen werden sicher auch ihre Lage hinterfragen: Sind meine Daten geschützt? Wer hat Zugriff auf meine Daten? Kann bei meinem Arbeitgeber eine ähnliche Panne auftreten oder kann man ihm vertrauen? Was darf und muss mein Chef über mich wissen? Diese Fragen werden schon durch die Köpfe vieler Arbeitnehmer gegangen sein, doch meist stößt man nur auf unsichere Antworten. In dieser Hausarbeit sollen die angesprochenen Probleme über den betrieblichen Datenschutz geklärt, die Rechte der Arbeitgeber und -nehmer beleuchtet und mögliche Konsequenzen aus fehlerhaftem Verhalten dargelegt werden.

2. Informationelle Selbstbestimmung - Grundlage des Datenschutzes

Im §1 (1) des Bundesdatenschutzgesetzes wird genau festgelegt, welches Recht jeder einzelne besitzt: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ [1] In anderen Worten verfasst bedeutet dies, dass jeder Einzelne vor dem Missbrauch seiner Daten in Form der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe geschützt werden soll. 1983 wurde dieses Recht auch vom Bundesverfassungsgericht als ein Grundrecht anerkannt.

3. Entstehung des Bundesdatenschutzgesetzes

Die Anfänge des BDSG gehen bis auf 1970 zurück. In dem besagten Jahr entstand in Hessen das erste Datenschutzgesetz der Welt. Es wurde z. B. festgelegt, dass persönliche Daten nicht weitergegeben werden dürfen, zum anderen entschied man sich für die Notwendigkeit eines Datenschutzbeauftragten, der bis heute wichtige Rolle spielt. Acht Jahre später wurde

[1] §1 (1) BDSG

schließlich auch das erste Bundesdatenschutzgesetz verabschiedet. Dieses wies zwar große Mängel auf, war jedoch ein weiter Schritt auf dem richtigen Weg. Nach weiteren fünf Jahren sollte eine geplante Volkszählung in Deutschland durchgeführt werden. Diese unterzog sich starker Kritik durch Proteste und Bürgerinitiativen und wurde schließlich durch das Bundesverfassungsgericht am 27. April untersagt. Das Gericht kritisierte in der Urteilsbegründung, dass eine Gesellschaftsordnung, in der der einzelne Bürger nicht mehr wissen könne, "wer was wann und bei welcher Gelegenheit" über ihn weiß, mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar sei.

1990 entstand schließlich das Bundesdatenschutzgesetz in der Form, in der wir es heute noch zum größten Teil kennen. Zum einen wurde die Rechtstellung Betroffener gestärkt, zum anderen wurde auch die die Nutzung und Erhebung von personenbezogenen Daten mit einer expliziten Zweckbindung erweitert. Im Laufe der Zeit bis heute wurden noch drei grundlegende Novellen hinzugefügt, um mit dem Fortschritt in der Technik und deren Anforderungen mitzuhalten.

4.1. Mitarbeiterdatenschutz - Allgemein

Bei den großen Datenskandalen, wie bei Lidl und der Bahn, waren immer die eigenen Angestellten die Betroffenen. Da stellt sich die Frage, wie mit dem Mitarbeiterdatenschutz umgegangen wird. Explizit wurde dieser Teil in noch keinem Abschnitt im BDSG oder in einem eigenen Gesetz geregelt. Daher kommt es wahrscheinlich auch zu diesen offensichtlichen Problemen. Schon vor den Bundestagswahlen 2009 lag dem ehemaligen Bundesinnenminister Olaf Scholz ein Gesetzesentwurf für einen eigenen Abschnitt im Bundesdatenschutzgesetz vor. Dieses Thema floss anschließend auch in den Koalitionsvertrag von CDU/CSU und FDP ein. Um Bespitzelung am Arbeitsplatz zu unterbinden, wie es bei Lidl der Fall war, sollen Arbeitgeber nur für das Arbeitsverhältnis erforderliche Daten verarbeiten dürfen. Im Gegenzug sollen sie „verlässliche Regelungen für den Kampf gegen Korruption an die Hand“[2] bekommen. Wann genau dieses Kapitel in das BDSG einfließt, ist noch nicht absehbar.

Trotz dieses fehlenden Abschnitts gibt es schon einige Passagen, die sich um den Arbeitnehmerdatenschutz kümmern. Zum einen findet man im Bundesdatenschutzgesetz Paragraph 32 Angaben darüber, wann personenbezogene Daten für das für das Beschäftigungsverhältnis erhoben, verarbeitet und genutzt werden dürfen. So ist dies zum Beispiel möglich, wenn ohne diese Daten das Arbeitsverhältnis nicht aufrecht erhalten werden könnte oder wenn es um die Aufdeckung von verdächtigen Straftaten mit tatsächlichen Anhaltspunkten nötig ist. Weitere Informationen zum Mitarbeiterdatenschutz sind auch im Betriebsverfassungsgesetz, Telemediengesetz, Telekommunikationsgesetz, Personalvertretungsgesetz, in der Bildschirmverarbeitungsordnung und in speziellen

[2] http://www.golem.de/0910/70684-2.html 24.01.10

Betriebsvereinbarungen nieder geschrieben. Jedoch kann man sagen, dass sie dieses Thema nur lückenhaft regeln, was am Ende wieder die Notwendigkeit des eigenen Kapitels im Bundesdatenschutzgesetz verstärkt. Bei vielen Streitpunkten, die noch nicht eindeutig im Gesetz festgelegt sind, spielen die Entscheidungen von Arbeitsgerichten eine entscheidende Rolle, denn oft werden diese als Maß herangezogen oder als Vorlage genutzt.

4.2. Mitarbeiterdatenschutz – Leistungs- und Verhaltensprofile

Trotz vieler Bedenken sind solche angelegten Profile nicht gesetzeswidrig sind, solange der Arbeitgeber ein berechtigtes Interesse aufweisen kann und er dabei die Rechte seines Angestellten nicht oder nur geringfügig verletzt. Automatisiert dürfen sie nur mit Zustimmung des Personalrats angelegt werden, wenn der Betroffene davon Kenntnis erhalten hat. Des Weiteren dürfen Daten, die dem Arbeitsverhältnis dienen und öffentlich zugänglich sind auch ohne Benachrichtigung erhoben, verarbeitet und genutzt werden. Darunter befinden sich Kriterien wie Geschlecht, Familienstand, Schulausbildung und dazugehörige Abschlüsse, Berufsausbildung und dazugehörige Abschlüsse, Sprachkenntnisse und krankheitsbedingte Fehlzeiten.

Der Nutzen von Leistungs- und Verhaltensprofilen liegt auf der Hand. Angestellte können effizienter im Betrieb nach ihren Qualifikationen eingesetzt werden, Arbeitszeiten können besser eingeteilt und verteilt werden, Mitarbeiter mit bestimmten Sprachkenntnissen können besser auf ausländische Kunden eingehen und es kann eine korrekte Lohn- oder Gehaltsabrechnung durchgeführt werden.

4.3. Mitarbeiterdatenschutz – Telefonüberwachung

Allgemein das Abhören am Arbeitsplatz ist nach §201 StGB strengstens untersagt und wird mit einer Geld- oder Freiheitsstrafe von bis zu 3 Jahren geahndet. Dabei spielt es keine Rolle, ob dies durch Abhörgeräte oder Tonbandaufnahmen geschieht. Man unterscheidet auch kein persönliches Gespräch oder geschäftliches Telefonat.

Im Gegensatz dazu muss man das Mithören von Telefongesprächen zum Abhören unterscheiden, denn das Mithören ist in der Regel nicht strafbar, solange das Persönlichkeitsrecht eines Gesprächspartners nicht verletzt wird. Dabei ist es auch irrelevant, ob es sich um ein Dienst- oder Privatgespräch handelt, denn nach dem Bundesverfassungsgericht unterliegt auch das dienstliche Telefongespräch dem Schutz des Allgemeinen Persönlichkeitsrechts.

In der Praxis werden die Gesprächsteilnehmer aufgrund dieser Rechtslage vor dem Gespräch aufgeklärt, dass das Telefonat mitgehört wird und dass sie ihr Einverständnis dazu geben. Mit diesem Einverständnis liegt der Arbeitgeber auf der sicheren Seite und geht kein Risiko ein.

5.1. Kundendatenschutz – positive Seite

Ein positiver Aspekt, der vielen Unternehmen im Bereich des betrieblichen Datenschutzes gutgeschrieben werden kann, ist der Kundendatenschutz, denn viele Betriebe investierten von sich aus viel Geld um das Persönlichkeitsrecht ihrer Kunden zu wahren. Natürlich stand dies auch im Sinne des Images des Unternehmens. Manchmal ist es jedoch unausweichlich und geschäftsmäßige Daten müssen erhoben und gespeichert werden. Der Kunde muss jedoch über die Erhebung, Speicherung und Übergabe benachrichtigt werden und der entsprechende Zweck ist ihm mitzuteilen.

5.2. Kundendatenschutz – Handel mit Kundendaten

Wer kennt es nicht? Telefon- oder Internetwerbungen versprechen ständig Preise, weil man der zehntausendste Besucher oder Kunde ist. Meist wird man bei den Telefongesprächen auch persönlich angesprochen, woraus sich die Frage ergibt: woher hat dieses Unternehmen diese Informationen?

Man muss klar unterscheiden zwischen legalem und illegalem Adresshandel. Der legale Handel beginnt mit dem Sammeln von Daten aus öffentlichen Quellen, zum Beispiel Gelbe Seiten und dem Telefonbuch. Diese Informationen sind nicht mehr schutzwürdig und können daher genutzt werden. Nimmt man an einem fragwürdigen Gewinnspiel teil, gibt man in der Regel seine Adresse und Telefonnummer preis für eventuelle Rückfragen oder Gewinnbenachrichtigungen. Stimmt man nun noch den Allgemeinen Geschäftsbedingungen zu, ohne sich im Klaren zu sein, was diese beinhalten, kann man seine persönliche Daten schneller verkauft sehen, als einem lieb ist. Unternehmen haben die Möglichkeit in den AGBs festzulegen, dass sie von ihrer Benachrichtigungspflicht befreit sind, wenn Daten erhoben, gespeichert oder weitergeben werden. Nun ist es auf völlig legalem Wege möglich, ihre Adresse und Telefonnummer an Geschäftspartner weiterzuleiten. Ist dies eingetreten, hat man als Verbraucher kaum noch erfolgreiche Chancen, seine privaten Informationen aus den Datenbanken unzähliger Unternehmen zu entfernen. Natürlich hat man das Recht, seine Daten löschen zu lassen, doch man weiß nie, welche Firma noch darauf zugreifen kann. Man kann auch schriftlich von einem Unternehmen fordern, dass die Daten vertraulich zu behandeln sind und nicht weitergeben werden dürfen. Ist dies der Fall und die Firma tut dies dennoch, dann spricht man hier klar von Missbrauch und illegalem Handel mit Kundendaten. Da es sich

meist um ein sehr lukratives Geschäft handelt, nehmen viele Firmen mögliche Strafen und Bußgelder in Kauf.

Doch wie wehrt man sich als Verbraucher effizient? Prävention ist hier das deutliche Schlüsselwort. Man sollte lieber zweimal darüber nachdenken, welche Felder man wo ausfüllt. Eine gesunde Skepsis sollte man stets entwickeln. Des Weiteren sollte man sich immer das „Kleingedruckte“ und die Allgemeinen Geschäftsbedingung durchlesen, man weiß nie, wo sich noch ein verstecktes Hintertürchen befinden kann.

Abschließend kann man sagen, dass der Schutz der Kundendaten klar von der Art des Unternehmens abhängig ist. Einige verdienen ihr Geld mit dem Verkauf von Waren und Dienstleistungen, andere verkaufen dagegen ihre Daten.

6. Technisierung der Betriebe

Ein guter positiver wirtschaftlicher Aspekt für Firmen ist die Expansion im Bereich der Technik. Neue Entwicklungen strotzen vor neuen Möglichkeiten. Fast jeder Computer in den Unternehmen ist heutzutage mit einem lokalen Netzwerk oder dem Internet verbunden. Natürlich schürt das auch die Möglichkeiten für den Missbrauch. Der wichtigste Punkt für Unternehmen sollte daher der Grundsatz der Datensparsamkeit sein.
Datenverarbeitungssysteme haben sich an dem Ziel zu orientieren, keine oder so wenig personenbezogene Informationen wie möglich zu erheben oder zu nutzen. Besonders automatisierte Verarbeitungsvorgänge werden angegriffen: die Datensammlungen sind gut verpackt und sortiert, sie schreien regelrecht danach geklaut zu werden.

Unternehmen sollten nicht an der falschen Stelle sparen. Software zur Pseudonymisierung oder Verschlüsslung der Daten ist zwar teuer und benötigt hohen technischen Aufwand, liefert am Ende jedoch eine sichere Möglichkeit Daten automatisiert zu verarbeiten. Natürlich kann damit ein hundertprozentiger Schutz nicht gewährleistet werden, wie sonst käme es zum Beispiel bei der Telekom zum Datenklau im großen Stile, jedoch ist es ein notwendiger Schritt. Deshalb sollte auch das Prinzip der Datensparsamkeit an erster Stelle stehen: wo keine Daten sind, können auch keine geklaut werden.

7.1. Grenzen der Datensicherung – für Geschäftszwecke

Natürlich kommen Unternehmen komplett ohne das Speichern von Kunden- oder Mitarbeiterdaten nicht aus. Für Geschäftszwecke dürfen diese Informationen gesichert, genutzt und verarbeitet werden, falls dies für ein rechtsgeschäftliches Schuldverhältnis erforderlich ist, wenn es um die Wahrung berechtigter Interessen der verantwortlichen Stelle

geht, die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen darf. Allerdings muss bei diesen Interessen stets der Zweck angegeben werden. [3]

Für einen anderen Zweck ist die Verarbeitung oder Nutzung personenbezogener Daten auch zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten, zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder für die Durchführung einer wissenschaftlichen Forschung einer Forschungseinrichtung erforderlich ist.[4]

Des Weiteren können die Daten genutzt und verarbeitet werden, wenn dem Zwecke der Werbung, Markt- oder Meinungsforschung dient und es sich um listenmäßig oder sonst zusammengefasste Daten über Angehöriger einer Personengruppe handelt, die sich auf

a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
b) Berufs-, Branchen- oder Geschäftsbezeichnung,
c) Namen,
d) Titel,
e) akademische Grade,
f) Anschrift und
g) Geburtsjahr

beschränken.[5]

Bei den Absätzen zwei und drei ist jedoch zu beachten, dass kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

7.2. Grenzen der Datensicherung – Rechte der Betroffenen

Möchte eine Person, dass seine Daten für Werbung, Markt- und Meinungsforschung nicht verarbeitet oder genutzt werden, egal aus welcher Quelle die Informationen stammen, so kann man bei der verantwortlichen Stelle widersprechen. Außerdem muss der Betroffene stets über den Zweck des Speicherns informiert werden, sei es der Grund für die Werbung, Markt- und Meinungsforschung oder des rechtsgeschäftlichen Schuldverhältnisses. Nutzt ein Betrieb eine andere Quelle der Daten, muss sichergestellt werden, dass die betroffene Person die Herkunft erfahren kann.[6] Die dazugehörigen Strafen, bei etwaigen Vergehen, werden im Kapitel *Grenzen der Datensicherung – Strafen* behandelt.

[3] §28 (1) BDSG
[4] §28 (2) BDSG
[5] §28 (3) BDSG
[6] § 28 (4) BDSG

7.3. Grenzen der Datensicherung – speziell für Markt- und Meinungsforschung

Für diesen Zweck ist das Nutzen und Speichern personenbezogener Daten nur erlaubt, wenn kein Grund der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss hat, oder wenn die Daten aus allgemein zugänglichen Quellen entnommen wurden[7], was sich zum Beispiel auf das Telefonbuch oder Gelbe Seiten bezieht. Diese Daten dürfen auch nur ausschließlich für dieses Forschungshaben verwendet werden. Werden sie allerdings stark anonymisiert, sodass kein Personenbezug mehr möglich ist, dürfen sie auch für einen anderen Zweck genutzt werden.[8] Außerdem müssen die Daten auch anonymisiert werden, sobald es das Forschungsvorhaben zulässt und kein Personenbezug mehr erforderlich ist.[9]

7.4. Grenzen der Datensicherung – Strafen

Natürlich müssen auch Strafen gegen Täter, die zuwider dem Bundesdatenschutzgesetz handeln, verhängt werden. Diese wurden auch im selbigen Gesetzbuch nieder geschrieben. Wer entgegen § 28 (4) Satz 2 BDSG den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann[10], der kann mit einer Geldbuße bis 50.000 Euro bestraft werden. Wer gegen § 28 (4) Satz 1 Daten für Werbung, Markt- und Meinungsforschung nutzt[11], der kann eine Geldbuße bis zu 300.000 Euro erhalten. Die Beträge sind allerdings nur als Richtlinie zu betrachten, denn wenn sie den Vorteil aus der Ordnungswidrigkeit nicht überschreiten, können problemlos überschritten werden. Verstößt man gegen § 43 (2) vorsätzlich für ein Entgelt, versucht man sich oder einen anderen zu bereichern oder den Betroffenen zu schädigen, dann ist sogar eine zweijährige Freiheitsstrafe möglich.[12]

Auf den ersten Blick wirken die Zahlen ziemlich groß, doch kann man sie in der Realität als „Peanuts“ betrachten. Vergleicht man zum Beispiel die Strafe der Bespitzelungsaffäre bei der Bahn in Höhe von 1,12 Millionen Euro zum Konzernumsatz 2008 von 33,452 Milliarden Euro, so wirkt dieses Bußgeld wie ein winziger Nadelstich. Nur den Imageschaden könnte man in diesem Fall als ernstzunehmende Strafe betrachten.

[7] § 30 (1) BDSG
[8] § 30 (2) BDSG
[9] § 30 (3) BDSG
[10] § 43 (1) 3. BDSG
[11] § 43 (2) 5b. BDSG
[12] § 44 (1) BDSG

8. Betrieblicher Datenschutzbeauftragter – Hinführung

Wird der Datenschutz in den Betrieben nicht ernst genommen und nur flüchtig betrachtet, so kann dies schnell zu Problemen führen. Auch aus technischer Sicht kann der kleinste Fehler große Lücken bei der Sicherheit hinterlassen. Doch wie können Unternehmen dem vorbeugen? Eine Methode, die in der Praxis auch häufig genutzt wird, wäre die Bestellung eines betrieblichen Datenschutzbeauftragten.

Betriebe können einen Datenschutzbeauftragten in schriftlicher Form bestellen oder sind sogar bei 10 beschäftigten Personen im Bereich der automatisierten Datenverarbeitung oder bei 20 beschäftigten Personen, die die Daten anders verarbeiten, dazu verpflichtet. Mit einer Bestellung ist man in der Regel auf der sicheren Seite, erfolgt keine, obwohl es Pflicht war, so droht ein Bußgeld aufgrund einer Ordnungswidrigkeit. Der betriebliche Datenschutzbeauftragte soll die Unternehmen bei rechtlichen, technischen und organisatorischen Problemen unterstützen. Genau genommen soll er für die Einhaltung des BDSG oder anderer Vorschriften über den Datenschutz sorgen. Er muss die ordnungsgemäße Anwendung der Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden, überwachen. Die Mitarbeiter, die in diesem Bereich tätig sind, sollen durch ihn geschult werden, zum Beispiel in schriftlicher Form, durch Veranstaltungen oder durch Anregungen und Informationen im Rahmen von Dienstbesprechungen. Vor Beginn der automatisierten Verarbeitung muss er kontrollieren, ob die Verarbeitung besondere Risiken für die Rechte der Betroffenen aufweist und diese eventuell beheben.

9. Quellen

www.golem.de/0910/70684-2.html 24. 01. 2010 - Koalitionsvertrag zu Internet, Datenschutz und IT

www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf 24. 01. 2010 - Bundesdatenschutzgesetz (BDSG)

Zur Vertiefung sind folgende Bezugsquellen zu empfehlen:

http://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung 24. 01. 2010 - Informationelle Selbstbestimmung

http://datensicherheit.oclink.de/seiten/datenschutzbeauftragter.shtml 24. 01. 2010 - Betrieblicher Datenschutzbeauftragter

http://www.bwr-media.de/themen/datenschutz/betrieblicher-datenschutz/ 24. 01. 2010 - BWR-Media News zum betrieblichen Datenschutz

http://de.wikipedia.org/wiki/Arbeitnehmerdatenschutz 24. 01. 2010 - Arbeitnehmerdatenschutz

http://www.pcwelt.de/start/sicherheit/backup/praxis/186255/der_glaeserne_mitarbeiter/ 24. 01. 2010 - Der gläserne Mitarbeiter

www.bewerbungsmappen.de/links/ArbeitsrechtXVIII/Arbeitsrecht209/arbeitsrecht209.html 24. 01. 2010 - Telefonüberwachung