DISKUSSIONSBEITRÄGE

aus dem

Fachbereich

WIRTSCHAFTSWISSENSCHAFTEN

der

UNIVERSITÄT DUISBURG - ESSEN
Campus Essen

Nr. 131
Dezember 2003

Das neue Datenschutzrecht

in der betrieblichen Praxis

Andreas Kladroba

Andreas Kladroba

Das neue deutsche Datenschutzrecht in der betrieblichen Praxis

1. Einleitung

Das deutsche Datenschutzrecht hat in den letzten Jahren einige einschneidende Veränderungen erfahren. Vor allem die Novellierung des Bundesdatenschutzgesetzes (BDSG) vom 23.05.2001 hat wichtige Neuerungen hervorgebracht. Hervorgerufen durch die Liberalisierung des Telekommunikationsmarktes sind außerdem einige Gesetze in Kraft getreten, die nicht nur für die Anbieter von Telekommunikation sondern vor allem auch für Unternehmen, die ihre Produkte über das Internet vertreiben, von besonderer Bedeutung sind. Hier sind zu nennen

1. *Telekommunikations-Datenschutzverordnung (TDSV)*: Sie ist als Nachfolgerin der Telekommunikationsdienstunternehmen-Datenschutzverordnung vom 12.07.96 am 18.12.2000 beschlossen worden. Ihr Anwendungsbereich ist der „Schutz personenbezogener Daten der an der Telekommunikation Beteiligten“ (§1 Abs. 1 Satz 1 TDSV), d.h. hier werden Datenschutzprobleme, die sich aus der Bereitstellung der entsprechenden technischen Einrichtungen ergeben, behandelt.[1]
2. *Teledienstdatenschutzgesetz (TDDSG)*: Das TDDSG ist als Art. 2 des Informations- und Kommunikationsdienstgesetzes (IuKDG) am 22.07.1997 verabschiedet worden. Sein Anwendungsbereich ist der „Schutz personenbezogener Daten bei Telediensten“ (§1 Abs. 1 TDDSG). Was unter einem Teledienst zu verstehen ist, regelt §2 Abs. 1 + 2 des Teledienstgesetzes (TDG) exemplarisch. Im Gegensatz zur TDSV wird im TDDG der inhaltliche Aspekt der Telekommunikationsnutzung behandelt. Darunter fallen auch Anwendungen wie Telebanking, E-Business u.ä.. Wichtig ist, dass es sich bei Telediensten um die individuelle Nutzung von Daten[2] handelt. Das unterscheidet Teledienste von Mediendiensten.
3. *Mediendienststaatsvertrag (MDStV)*: Der am 01.07.1997 in Kraft getretene MDStV gilt „für das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten“ (§2 Abs. 1 MDStV).

[1] zu Einzelheiten vgl. z.B. Koenig/Neumann (2000), Schild (2000 a + b)
[2] vgl. Bizer (1998), S. 277

Dabei besteht das Problem, dass die Grenzen zwischen den Anwendungsbereichen oftmals fließend sind. Vor allem die Unterscheidung zwischen Tele- und Mediendiensten fällt oftmals schwer. Erleichtert wird dieses Problem dadurch, dass die Datenschutzbestimmungen von TDDSG und MDStV quasi identisch sind. Problematischer ist dagegen der Übergang zwischen den Geltungsbereichen von TDDSG/MDStV auf der einen und BDSG auf der anderen Seite. Ein typisches Beispiel ist das Telebanking. Nimmt ein Kunde Bankgeschäfte über das Internet vor, gelten die Vorschriften des TDDSG, tätigt er aber die gleichen Geschäfte am Schalter seiner Bank, fallen diese in den Geltungsbereich des BDSG.

Datenschutz ist der Schutz sogenannter „personenbezogener Daten". Darunter versteht man „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" (§3 Abs. 1 BDSG). Personenbezogene Daten fallen im Unternehmen vor allem in Form von Mitarbeiter- und Kundendaten an.

Dabei sind Mitarbeiterdaten in den meisten Fällen von den beschriebenen Gesetzesänderungen nicht betroffen. Da das BDSG anderen Gesetzen prinzipiell nachgelagert ist, greifen in diesem Bereich zunächst eine ganze Reihe unterschiedlicher Vorschriften. Dies sind beispielsweise:[3]

- das Betriebsverfassungsgesetz bezüglich des Inhalts von Personalfragebögen und des Umgangs mit Personalakten oder
- das Sozialgesetzbuch, die Reichsversicherungsordnung, die Zivilprozessordnung und die verschiedenen Steuergesetze und –verordnungen bezüglich der Weitergabe von Arbeitnehmerdaten an Sozialversicherungsträger, die Bundesanstalt für Arbeit, Gläubiger im Zwangsverfahren, Finanzbehörden usw.

Neben diesen „klassischen" Personaldaten fallen durch die Verwendung moderner Arbeits- und Kommunikationsmittel (PC, Telefon usw.) in vielen Unternehmen weitere Daten an, die von den Datenschützern kritisch beobachtet werden, weil „dem Arbeitgeber so ein umfassender Überblick und letztlich eine breite Palette von Handlungs- und Bewertungsmöglichkeiten im Hinblick auf die Beschäftigten" zukommt, was zu einer „Machtverschiebung zugunsten des Arbeitgebers"[4] führen kann. Aber auch hier greift in der Regel das BDSG nicht, weil solche Probleme meist im Rahmen von Betriebsvereinbarungen auf der Basis von §87 Abs. 1 Nr. 6 BetrVG innerbetrieblich geregelt werden. Solche Betriebsvereinbarungen gelten ebenso als übergeordnete Rechtsvorschriften im Sinne des §4 Abs. 1 BDSG wie die oben bereits erwähnten Gesetze und Verordnungen.

Die einschlägigen Datenschutzvorschriften wie BDSG und TDDSG finden daher auch eher Anwendung auf Kundendaten. Dieser Bereich hat sich vor allem mit der Einführung von

[3] o.V. (1989), Bartosch (1992), Koch (1997)

Kundenkarten und der verstärkten Geschäftsabwicklung über das Internet in den vergangen Jahren stark verändert.

Die vorliegende Arbeit möchte die relevanten Gesetzesänderungen kurz mit einigen Implikationen für private Unternehmen vorstellen. Dabei behandelt Kap. 2 zunächst das neue Bundesdatenschutzgesetz, während Kap. 3 sich mit dem Datenschutz im Internet auseinandersetzt.

2. Das neue BDSG

Am 24.10.1995 hat die Europäische Kommission die EG-Datenschutzrichtlinie 94/46/EG verabschiedet. Die vorgesehene Drei-Jahres-Frist zur Umsetzung in nationales Recht ist in Deutschland allerdings ungenutzt verstrichen, was der damaligen Bundesregierung viel Kritik von Seiten der Datenschützer eingebracht hat. Erst am 11.05.2001 nahm das neue BDSG die letzte parlamentarische Hürde.

Verglichen mit dem alten BDSG stellt die Novelle deutlich strengere Anforderungen an den Datenschutz. Man kann zwei Veränderungen beobachten:

1. Verschärfung bereits bestehender Vorschriften
2. Einführung neuer Vorschriften.

Im folgenden sollen kurz die wichtigsten Änderungen des BDSG und deren Implikationen für private Unternehmen aufgezeigt werden.[5]

2.1 Verschärfungen

Folgende Vorschriften sind im neuen BDSG strenger gefasst als im Alten:

1. Gemäß der alten Fassung des BDSG war die Datenverarbeitung durch nicht-öffentliche Stellen einzig für gewerbliche Zwecke verboten. Andere Verwendungen waren dagegen erlaubt. Die neue Fassung erlaubt nur noch die Verwendung ausschließlich für private Zwecke (§1 Abs. 2 Nr. 3 BDSG).
2. Das neue BDSG setzt an vielen Stellen die „verantwortliche Stelle“ statt der „speichernden/erhebenden Stelle“ (z.B. §13 Abs. 1, §14 Abs. 1, §19 Abs. 6). Unter verantwortlich versteht man dabei jede Stelle, „die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“ (§ 3 Abs. 7

[4] Wohlgemuth (1996), S. 690
[5] Die für den öffentlichen Bereich vorgenommenen Veränderungen sollen hier nicht weiter interessieren.

BDSG) Im Falle einer Datenverarbeitung im Auftrag führt dies zu einer viel stärkeren Verantwortlichkeit des Auftraggebers (§11 BDSG).

3. Eine völlige Neufassung hat §4 erfahren:

   - §4 Abs. 1 betont jetzt die Notwendigkeit der Erlaubnis zur Erhebung von Daten.[6] In der bisherigen Fassung wurde die Erlaubnis nur für die Verarbeitung und Nutzung benötigt.
   - Gemäß §4 Abs. 2 sind personenbezogene Daten ausschließlich beim Betroffenen zu erheben. Die von dieser Vorschrift gemachten Ausnahmen sind quasi nur in der amtlichen Statistik anwendbar.
   - §4a schreibt für die einzuholende Erlaubnis die Schriftform vor, was – wie wir noch sehen werden – im Internethandel zu einigen Problemen führt.
   - Die in diesem Paragrafen enthaltenen Vorschriften zur „automatisierten Verarbeitung" werden uns an späterer Stelle noch beschäftigen.

4. Die Möglichkeit von Schadensersatzleistungen an Betroffene wird erstmals auch für nicht-öffentliche Stellen explizit genannt (§7 BDSG). Im alten BDSG wird diese Möglichkeit zwar angedeutet (§8 BDSG-alt), in der Neufassung wurde aber erstmalig eine Anspruchsgrundlage dafür geschaffen.

5. Der Begriff der „allgemein zugänglichen Daten", der in der alten Fassung eher unklar formuliert war, wird in der neuen Fassung konkreter als „Daten, die jedermann, sei es ohne oder mit vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann" gefasst (§10 Abs. 5 BDSG).

6. Ebenso eine Verdeutlichung erfährt die Forderung nach „zweckgerichteten Erhebungen". Herrschte im Datenschutz auch bisher ein Konsens darüber, dass die Erhebung von Daten immer einem bestimmten Zweck zu dienen hat und dass eine Erhebung „auf Vorrat" unzulässig ist, wird dies jetzt explizit betont (§28 Abs. 1 Satz 2)

7. Eine deutlich höhere Hürde als vorher stellt das neue BDSG für Werbemaßnahmen bzw. Markt- und Meinungsforschung auf. Zwar gilt nach wie vor die Regelung des §28 Abs. 4 (vorher Abs. 3), dass Daten von Betroffenen, die einer Verwendung ihrer Daten für diese Zwecke widersprechen, eben auch nicht verwendet werden dürfen, allerdings sind diese jetzt bei der Ansprache explizit auf das Widerspruchsrecht aufmerksam zu machen. Eine

[6] Die Erhebung von Daten wird im allgemeinen viel stärker angesprochen als vorher (vgl. z.B. §5, §9 Abs. 1, §11).

Ansprache in der Hoffnung, dass dem Betroffenen diese Regelung nicht bekannt ist,[7] ist somit nicht mehr möglich.

2.2 Neu eingeführte Vorschriften

An neu eingeführten Vorschriften sind vor allem zu nennen:

1. Als neue Datenschutzgrundsätze wurden Datensparsamkeit und Datenvermeidung eingeführt. Es ist allerdings zu befürchten, dass diese Grundsätze als nicht mehr als ein frommer Wunsch anzusehen sind. Es dürfte kaum einer verantwortlichen Stelle nachzuweisen sein, dass sie gegen diese Grundsätze verstößt. Der Datenschutz ist hier einzig auf den guten Willen der Unternehmen angewiesen.
2. Es hat eine starke Konkretisierung des Begriffs der „automatisierten Verarbeitung" stattgefunden. Gemäß der neu geschaffenen Definition in §3 Abs. 2 versteht man unter einem automatisierter Verarbeitung „die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen". Neu ist ebenfalls, dass für die automatisierte Verarbeitung vor ihrer Inbetriebnahme eine Meldepflicht bei der zuständigen Aufsichtsbehörde besteht (§4d Abs. 1 BDSG). Auf diese kann verzichtet werden, wenn die Stelle eines Datenschutzbeauftragter eingerichtet ist oder diese Form der Datenverarbeitung nur für eigene Zwecke von einem kleinen, genau definierten Mitarbeiterkreis vorgenommen wird. Als besonders problematisch wird dabei die Verarbeitung von personenbezogenen Daten der sogenannten „besonderen Art" gem. §3 Abs. 9 BDSG[8] angesehen (§4d Abs. 5 BDSG). Diese Anwendungen sind einer Vorabkontrolle durch die Aufsichtsbehörde zu unterziehen. Das gleiche gilt, wenn die Erhebung der Bewertung der Persönlichkeit des Betroffenen einschließlich seiner Fähigkeiten und Leistungen dient.
3. Ähnlich eingeschränkt wird die Möglichkeit mit Hilfe einer automatisierten Entscheidungen zu treffen, wenn diese „für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen" (§6a Abs. 1BDSG). Solche Entscheidung dürfen nicht alleine auf die automatisierte Verarbeitung gestützt sein. Außerdem ist der Betroffene in die Entscheidung einzubeziehen. Eine Ausnahme stellt der Fall dar, bei dem die Entscheidung im Sinne des Betroffenen ausfällt. Von besonderer Bedeutung dürfte diese Vorschrift z.B. für die Kreditvergabe von Banken sein, wenn eine Kreditentscheidung einzig mit Hilfe eines Scoringsystems getroffen wird, das die Kreditnehmer anhand unterschiedlicher Merkmale in „kreditwürdig" und „nicht kreditwürdig" unterteilt.

[7] Eine Vorgehensweise, die man sicherlich ruhigen Gewissens einigen Unternehmen unterstellen kann.
[8] Dabei handelt es sich vor allem um Daten der persönlichen Überzeugung.

4. §9a sieht erstmals die Möglichkeit eines Datenschutzaudits für Unternehmen vor. Darin sollen die Datenschutzanstrengungen des Unternehmens von externen Gutachtern bewertet und schließlich zertifiziert werden. Eine genaue gesetzliche Ausgestaltung steht allerdings noch aus. In Folge des vierten Zwischenbericht der Bundestags-Enquête-Kommission „Zukunft der Medien“ (BT-Drs. 13/11002) herrscht in der aktuellen Diskussion allerdings der Konsens, dass die Ausgestaltung eines Datenschutzaudits an das in der Bundesrepublik bereits seit einigen Jahren existierende Umweltaudit angelehnt werden sollte. Zur Diskussion um die Ausgestaltung sei an dieser Stelle auf die entsprechende Literatur verwiesen.[9]

3. Datenschutz im Internet

Die folgenden Betrachtungen über „Datenschutz im Internet“ beschränken sich einzig auf den Bereich des E-Business, also auf den Fall, dass Unternehmen ihre Produkte über das Internet vertreiben. Unternehmen, deren Ziel die Bereitstellung des Internets selber ist, also Telekommunikationsunternehmen oder Service-Provider, sollen hier außen vor bleiben.

Die Diskussion über Datenschutz und Internet wird mit einer immer weiter zunehmenden Nutzergemeinde auch für immer mehr Menschen interessant. Dabei ist die Meinung, die Angebote würden oftmals nicht den Rechtsvorschriften entsprechen, weit verbreitet.[10] Auch entsprechende Presseberichte unterstützen diese Ansicht.[11] Dabei ist die Annahme sicherlich nicht zu weit hergeholt, dass bei vielen Unternehmen einfach eine gewisse Unkenntnis und somit auch Sorglosigkeit bezüglich der Datenschutzproblematik diagnostiziert werden kann.

Der wichtigste Unterschied zwischen dem Handel im Internet und dem Handel mit Hilfe von Verkaufsstellen besteht bezüglich des Datenschutzes darin, dass hier zwei Formen von Daten anfallen.

Zunächst handelt es sich hier um ein Fernabsatzgeschäfte, d.h. zur Erfüllung des Kaufvertrags müssen im Regelfall mehr Daten vorliegen als beim stationären Handel. Diese Daten sind z.B. Name und Anschrift des Käufers. Insofern unterscheidet sich E-Business nicht von einem Geschäft, das z.B. mit Hilfe eines Katalogs und einer Bestellkarte oder einem Telefonanruf erfolgt. Die Aufnahme dieser Daten ist gem. §28 Abs. 1 BDSG auch entsprechend unproblematisch.[12] Dementsprechend sind auch die in diesem Fall anzuwendenden Vor-

[9] Arbeitskreis „Datenschutzbeauftragte“ (1999), Drews/Kranz (1998), Gola (2000), Königshofen (2000), Roßnagel (1997)
[10] Wolters (1999), Gundermann (2000)
[11] z.B. Capital 18/2000, S. 127 – 128, Wirtschaftswoche 7/2000, S. 103 – 106 und Wirtschaftswoche 33/2000, S. 75 – 78
[12] Auch wenn hier nach einer Untersuchung von Wolters (1999) bereits einige Unternehmen deutlich über das Ziel hinausschießen.

schriften des TDDSG denen des BDSG sehr ähnlich und sollen hier nicht weiter behandelt werden.

Darüber hinaus fallen aber auch Daten an, die sich aus der Verwendung der Internettechnologie ergeben (können). Zum Beispiel wird auf dem Anbieterserver automatisch die IP-Adresse des Kunden gespeichert, sowie die Häufigkeit seines Besuchs und die Verweildauer auf einzelnen Seiten. Zumindest theoretisch ist es möglich, diese Information zur Erstellung eines Kundenprofils zu nutzen.

Allerdings kennzeichnet die IP-Adresse zunächst nur einen bestimmten Rechner und nicht eine bestimmte Person. Somit ist die IP-Adresse kein personenbezogenes Datum und ihre Speicherung und Verarbeitung datenschutzrechtlich unproblematisch. Erst die Zusammenführung einer IP-Adresse mit einer bestimmten Person macht daraus ein personenbezogenes Datum. Diese Zusammenführung funktioniert aber nur in Ausnahmefällen und kann in der Regel nur vom Administrator des Kunden geleistet werden. Das E-Business-Unternehmen wäre also auf eine entsprechende Zusammenarbeit angewiesen. Darüber hinaus haben viele Kunden einen Internet-Zugang über einen Provider. Diese verfügen in der Regel aber nicht über genug IP-Nummern, dass jedem Kunden eine feste Adresse zugeordnet werden kann. Es werden somit dynamische IP-Adressen vergeben, d.h. der Nutzer bekommt bei jeder Anmeldung eine neue IP. Damit wird eine direkte Zuordnung einer Person zu einer IP fast unmöglich gemacht. Im Falle einer festen IP, wie sie z.B. von Universitäten vergeben werden, ist die Zuordnung zu einer Person relativ leicht, wenn nur eine Person einen bestimmten Computer benutzt. Die Zuordnung kann dann z.B. einfach über ein vom Nutzer ausgefülltes Produkt-Bestellformular erfolgen.

Ein weiteres, immer wieder in die Schlagzeilen geratenes technisches Instrument, sind sogenannte Cookies.[13] Dabei handelt es sich um Dateien, die von einem Web-Server auf der Festplatte eines Client-Rechners abgelegt wird und dort bestimmte Aufgaben erfüllen sollen. Cookies werden z.B. benötigt um sogenannte „Warenkörbe“ anzulegen, mit denen ein E-Business Kunde die Internet-Seiten des Anbieters durchsuchen und Waren, die er bestellen möchte, sammeln kann. Die Bestellung erfolgt schließlich als Sammelbestellung. Cookies können aber auch quasi als externer Datenspeicher genutzt werden um z.B. die Bewegungen des Nutzers im Internet aufzuzeichnen. Die Ergebnisse werden dann zu von den Nutzern nicht bekannten Zeitpunkten an den Server, der das Cookie gesetzt hat, oder einen anderen Server zurückgeschickt.

Datenschutzrechtlich problematisch ist dabei:

1. Der Nutzer kann zwar die Platzierung eines Cookies unterbinden, allerdings sind ihm dann oft wichtige Bereiche des Internetangebots verschlossen.

2. Die genaue Aufgabe, sowie die Lebensdauer eines Cookies sind dem Nutzer in der Regel unbekannt.
3. Der Zeitpunkt des Versendes des Cookies kann vom Nutzer nicht beeinflusst werden. Darüber hinaus hat er meist keine Information darüber, wohin der Cookie gesendet wird.

Das Setzen eines Cookies, das die Identifikation eines Nutzers ermöglicht, gilt in der Literatur allgemein als „speichern" von Daten.[14] Es gelten somit die Vorschriften des TDDSG über das Erheben und Nutzen von Daten:

1. Grundsatz der Datensparsamkeit (§3 Abs. 4 TDDSG)
2. Erlaubnisvorbehalt des Betroffenen (§3 Abs. 1 TDDSG) mit Widerrufsrecht (§3 Abs. 6 TDDSG) oder Datenerhebung zur Vertragserfüllung (§5 Abs. 1 TDDSG) bzw. soweit dies zur Bereitstellung und Abrechnung des Teledienstes nötig ist (§6 Abs. 1 TDDSG)
3. Verwertung der Daten zu Marketingzwecken nur nach ausdrücklicher Erlaubnis des Nutzers (§5 Abs. 2 TDDSG)
4. Auskunftsrecht des Nutzers (§7 TDDSG). Im Unterschied zu den entsprechenden Vorschriften des BDSG bezieht sich das Auskunftsrecht hier auch auf ein eventuell bestehendes Pseudonym.

Der Gesetzgeber hat den beiden hier beschriebenen technischen Anwendungsmöglichkeiten mit der neuen Datenschutzgesetzgebung relativ hohe Hürden gesetzt. So sind Nutzerprofile nur in pseudonymisierter Form erlaubt (§4 Abs. 4 TDDSG und §13 Abs. 4 MdStV). Des weiteren ist der Nutzer zu unterrichten, wenn automatisierte Verfahren angewandt werden, die eine Identifikation ermöglichen, wie das bei bestimmten Cookies der Fall ist (§3 Abs. 5 TDDSG). Es gilt allerdings die verbreitete Einschätzung, dass dieser Unterrichtungspflicht nur zögerlich nachgekommen wird.[15]

Eine weitere Besonderheit der Datensammlung im Rahmen eines E-Businessvorgangs besteht darin, dass die zur Erhebung, Verarbeitung und Nutzung von Daten notwendige Einwilligung des Betroffenen (§ 4 Abs. 1 BDSG) normalerweise der Schriftform bedarf, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist" (§4a Abs. 1 Satz 3 BDSG). Da eine schriftliche Erklärung im gesamten E-Business ein relativ großes Hindernis darstellen würde, erlaubt §3 Abs. 7 TDDSG unter recht strengen Restriktionen eine elektronische Einverständniserklärung. Wie diese genau ausgestaltet werden kann, wird im Augenblick noch diskutiert.

---

[13] zu Einzelheiten vgl. Wichert (1998), Bizer (1998), Gundermann (2000)
[14] vgl. z.B. Bizer (1998)
[15] vgl. Wolters (1999)

Über die hier beschriebenen Datenschutzprobleme hinaus bietet das Internet natürlich eine relativ weite Palette von Missbrauchsmöglichkeiten, die aber schon als kriminell zu bezeichnen sind und die daher auch nicht das Thema dieser Arbeit sind. Wolters (1999) führt dazu einige Beispiele an.

4. Fazit

Moderne Datenverarbeitungs- und Kommunikationstechniken haben einen grundlegenden Wandel des Datenschutzes innerhalb von Unternehmen erforderlich gemacht. Schapper (1988) hat z.B. noch zwischen sensiblen und weniger sensiblen Daten unterschieden, die eine unterschiedliche datenschutzrechtliche Behandlung erforderten. Es ist zweifelhaft, ob diese Unterscheidung heute immer noch gemacht werden kann, da die heutige Technologie ein relativ einfaches Zusammenführen auch extrem großer Datenmengen ermöglicht und so in Einzelfällen aus scheinbar „harmlosen“ Daten plötzlich hochsensible werden. Ein einfaches Beispiel mag dies unterstreichen: Angenommen an einer Supermarktkasse werden die Einkäufe des Kunden A registriert. Die Speicherung dieser Daten mag vielen als harmlos erscheinen. Ein einfaches Zusammenführen dieser Daten mit den Personaldaten unseres Unternehmens zeigt uns, dass Kunde A gleichzeitig Mitarbeiter des Unternehmens ist, der seine Einkäufe verbotenerweise während der Arbeitszeit getätigt hat, was für ihn schwerwiegende rechtliche Konsequenzen nach sich ziehen kann.

Wie bereits erwähnt ist die Novellierung des BDSG zunächst nur eine Anpassung an die Europäische Datenschutzrichtlinie gewesen. Eine zweite Novelle ist bereits geplant. Diese wird sich vermehrt um eine inhaltliche Anpassung des Datenschutzes an heutige Gegebenheiten bemühen müssen. In der modernen Welt leben Unternehmen mit zwei verschiedenen Aspekten der Datennutzung: Zum einen benötigen sie Informationen für eine effektive Unternehmensführung. Das gilt sowohl für Mitarbeiter- als auch für Kundendaten. Informationen sind somit heutzutage eine Ware geworden. Zum anderen gilt aber nach wie vor das Prinzip der Informationellen Selbstbestimmung. Der Datenschutz der Zukunft wird gut daran tun beide Aspekte sehr genau im Auge zu behalten.

Literatur

Arbeitskreis „Datenschutzbeauftragte“ im Verband der Metallindustrie Baden-Württemberg (1999), Datenschutz-Audit, in: Datenschutz und Datensicherheit 23, S. 281 - 283

Bizer, J. (1998), Web-Cookies – datenschutzrechtlich, in: Datenschutz und Datensicherheit 22, S. 277 - 281

Bartosch, D. (1992), Datenschutz im Personalwesen, in: Personalführung 10/92, S. 802 – 811

Büllesbach, A. (1999), Das TDDSG aus Sicht der Wirtschaft, in: Datenschutz und Datensicherheit 23, S. 263 - 265

Büllesbach, A. (2000), Datenschutz in globalen Unternehmen, in: Recht der Datenverarbeitung 16, S. 1 – 6

Drews, H.-L./H. J. Kranz (1998), Argumente gegen die gesetzliche Regelung eines Datenschutz-Audits, in: Datenschutz und Datensicherheit 22, S. 93 – 94

Gola, P. (2000), Der auditierte Datenschutzbeauftragte – oder von der Kontrolle der Kontrolleure, in: Recht der Datenverarbeitung 16, S. 93 - 96

Gundermann, L. (2000), E-Commerce trotz oder durch Datenschutz?, in: Kommunikation und Recht 5/2000, S. 225 – 235

Koch, F. (1997), Datenschutz-Handbuch für die betriebliche Praxis, 2. Auflage, Freiburg i. Breisgau

Koenig, Ch./A. Neumann (2000), Die neue Telekommunikations-Datenschutzverordnung, in: Kommunikation und Recht 9/2000, S. 417 – 425

Königshofen, T. (2000), Chancen und Risiken eines gesetzlich geregelten Datenschutzaudits, in: Datenschutz und Datensicherheit 24, S. 357 - 360

o.V. (1985), Datenschutz im Betrieb, in: Betriebs-Wirtschafts-Magazin 5/85, S. 10 – 14

o.V. (1989), Datenschutz im Unternehmen, in: Office Management 7-8/89, S. 14 – 16

Roßnagel, A. (1997), Datenschutz-Audit, in: Datenschutz und Datensicherheit 21, S. 505 - 515

Schapper, C. H. (1988), Datenschutz und Datensicherung beim betrieblichen Einsatz von Personalcomputern, in: Arbeit und Recht 4/88, S. 97 – 105

Schild, H.-H. (2000a), Die neue Telekommunikations-Datenschutzverordnung, in: Rtkom 3/2000, S. 211 – 220

Schild, H.-H. (2000b), Die neue Telekommunikations-Datenschutzverordnung: eine aktualisierende Ergänzung, in: Rtkom 4/2000, S. 262 - 263

Wohlgemuth, H. H. (1996), Auswirkungen der EG-Datenschutzrichtlinie auf den Arbeitnehmer-Datenschutz, in: Betriebs-Berater 13/96, S. 690 – 695

Wolters, S. (1999), Einkauf via Internet: Verbraucherschutz durch Datenschutz, in: Datenschutz und Datensicherheit 23, S. 277 - 280

Wichert, M. (1998), Web-Cookies – Mythos und Wirklichkeit, in: Datenschutz und Datensicherheit 22, S. 273 - 276