Auswirkungen des neuen Bundesdatenschutzgesetzes auf Unternehmen

Manfred Böttcher

Mit der Änderung des Bundesdatenschutzgesetzes im Jahr 2002 (Gesetz vom 21. August 2002;BGBl. I S. 3322) stellt sich erneut für viele Unternehmen die Frage des Datenschutzes. Es wurden eine Vielzahl von Regelungen aufgenommen, die der technischen und gesellschaftlichen Entwicklung Rechnung tragen. So wurden u. a. Regelungen für den Einsatz von Videoüberwachungsanlagen in das Gesetz eingearbeitet. Noch stärker, als schon im alten Gesetz finden sich Regelungen, die die Rechte der Betroffenen stärken.

Ein sehr großer Abschnitt beschäftigt sich mit der Übermittlung bzw. Verarbeitung von Daten, u. a. wird hier sehr dezidiert auf die sog. Auftragsverarbeitung (die jeder Normalbürger von seinen Arztrechnungen her kennt) eingegangen.

Besonders relevant ist zum einen die Frage nach der Behandlung von Kundendaten im e-commerce Bereich, zum anderen die Frage nach der Zulässigkeit der Weitergabe und Verteilung von Mitarbeiterdaten speziell in großen Organisationen (Holdingstruktur der Unternehmung).

Das Gesetz hat gerade in letztem Bereich einige deutliche Schranken gezogen. Dies ist eine Reaktion auf den vermehrten Einsatz von Personalinformationssystemen (Beispiel: SAP HR) in den Unternehmen.

So ist die Zulässigkeit der Übermittlung von Personendaten durch das Gesetz im Wesentlichen eingeschränkt auf 1. Mitgliedsstaaten der Europäischen Union und 2. „andere Vertragsstaaten" des Abkommens über den europäischen Wirtschaftsraum.

Im Gesetz wird festgelegt (ich zitiere, Hervorhebung von mir): „Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen **ein angemessenes Datenschutzniveau nicht gewährleistet ist**." Damit sind insbesondere Staaten gemeint, die internationalen Abkommen nicht beigetreten sind (vor allem sind hier die USA gemeint).

Wie problembeladen das ist, möchte ich an einem aktuellen Beispiel verdeutlichen, der Weitergabe von Fluggastdaten an amerikanische Zoll- und Grenzschutzbehörden:

„Die Kommission hat diese Frage in ihren bilateralen Kontakten mit den USA seit Dezember 2001 zur Sprache gebracht. Aufgrund dieser Kontakte hat die CBP den Fluggesellschaften, die sich auf ihre Verpflichtungen nach der EU-Datenschutzrichtlinie berufen, eine Fristverlängerung bis zum 5. März 2003 gewährt. Hochrangige Vertreter der Europäischen Kommission und der CBP (vormals US Customs) kamen am 17./18. Februar 2003 in Brüssel zusammen. Weitere Erörterungen fanden Ende Februar und Anfang März statt. Beide Seiten waren sich einig, auf eine bilaterale Vereinbarung hinzuarbeiten, die die US-Anforderungen mit den datenschutzrechtlichen Anforderungen in der EU in Einklang bringt, wonach die Kommission eine Feststellung nach Artikel 25 Absatz 6 trifft. Die Kommission ist außerdem der Auffassung, dass längerfristig eine multilaterale Übereinkunft im Rahmen der ICAO nötig ist, da es äußerst unpraktisch ist, wenn sich die Fluggesellschaften, die Daten in der EU erfassen und verarbeiten, nach ganz unterschiedlichen, einseitig auferlegten oder bilateral vereinbarten Anforderungen richten müssen. Die Gespräche zwischen der CBP und der Kommission dauern an. Die Kommission hat die europäische Luftverkehrsbranche in dieser Angelegenheit konsultiert."

(FAQ der Eu-Kommission zur Übermittlung von Fluggastdaten von der EU an die USA vom 12.3.2003 in Memo /03/53)

Man sieht, wie schwierig der ganze Prozess ist. Erschwert wurde er durch die Ereignisse des 11. September. Amerikanische Behörden haben seitdem deutlich die Befugnisse der Ermittlungsbehörden ausgedehnt.

Aber nicht nur der Problemfall USA macht Untersuchungen bzgl. des betrieblichen Datenschutzes notwendig, sondern auch die unterschiedlichen Regelungen im europäischen Raum. So kennt Deutschland nur die Schutzwürdigkeit **natürlicher Personen** im Gesetz, während Länder wie Dänemark auch eine Schutzwürdigkeit für **juristische Personen** festschreiben. Dies hat dann unmittelbare Auswirkungen auf die Verarbeitung und Weitergabe von Kunden- und Lieferantendaten, wodurch u. a. der gesamte e-commerce Bereich betroffen ist.

Damit ist klar, dass weitaus größere Bereiche von Fragen des Datenschutzes betroffen sind, als bislang. In diesem Zusammenhang wird verständlich, warum die Unternehmen eine Neubewertung ihrer Systeme vornehmen (müssen).

In den letzen Jahren wurde ein erneutes Audit der Systeme durch viele Unternehmen durchgeführt. Dies geschah – unter der oben beschriebenen Prämisse – aus mehreren Gründen:

Zum einen wurden bekannte, z.T. durch Wirtschaftsprüfungsgesellschaften wiederholt angesprochene Mängel beseitigt (z. B. zu häufige Verwendung des Rechtes „SAP_ALL" im ERP-System des Unternehmens). Dies wurde erleichtert durch die Tatsache, dass die ERP-Hersteller entsprechende Werkzeuge zur Untersuchung kritischer Rechte zur Verfügung stellen.

Zum anderen wurde von den Unternehmen die Gelegenheit genutzt, die gesamten Sicherheitsbereiche einer kritischen Sichtung zu unterwerfen. Dies betraf sowohl technische Einrichtungen (Stromversorgung, Zugangssysteme, Netzwerk….), als auch Ablaufprozesse, wie z. B.

Arbeitsanweisungen u. ä. Dies erstreckte sich bis hin zu Fragen der Sicherheit innerbetrieblicher Dokumente, mit besonderem Augenmerk auf die Frage der Wiederauffindbarkeit von Unterlagen.

Aus diesen Erfahrungen lassen sich Fragestellungen für ein Vorgehen im Datensicherheitsbereich ableiten, die den Forderungen des Datenschutzgesetzes genüge tun.

Vorschläge für ein Vorgehen

1. Ist das Unternehmen rein national tätig, oder international organisiert? Im ersten Fall brauchen nur die Bestimmungen des deutschen Datenschutzgesetzes beachtet zu werden.
2. Es muss eine Neuuntersuchung der verarbeitenden Systeme vorgenommen werden. Dies betrifft natürlich zuvorderst den Bereich Personalwesen; dort vor allem aber den Bereich Personalinformationssysteme. Insbesondere muss hier ein Augenmerk auf die Daten in den Mitarbeiterinformationsbereichen (wie z. B. Zielvereinbarungen…) gelegt werden. Hier zieht das Gesetz enge Grenzen, was die Weitergabe der Daten (z. B. an Abteilungsexterne) angeht. Es zeigen sich allerdings auch Möglichkeiten, so z. B. wenn der Vorgesetzte einem anderen Unternehmen angehört, dann sind Weitergaben zulässig. Dies ist besonders interessant für Unternehmen mit einer Holding Struktur.
3. Ich erwarte eine Ausdehnung der Betroffenengruppen in Richtung Hinzunahme von juristischen Personen in den Datenschutz. Damit wäre ein Schritt in Richtung der Vereinheitlichung von Gesetzen getan. Es ist also sinnvoll, in diesem Zusammenhang die Verarbeitung von Kunden- und Lieferantendaten im Vertrieb einer Überprüfung zu unterziehen. Unmittelbar notwendig ist die Bearbeitung der AGB´s in den e-commerce Bereichen des Unternehmens. Ein sehr gutes Beispiel hierfür sind die AGB´s von ebay.
4. Ebenfalls sinnvoll (und wahrscheinlich in absehbarer Zeit Pflicht) ist die Durchführung eines Datenschutz-Audits mit anschließender Zertifizierung. Das Bundesdatenschutzgesetz weist bereits im §9a auf eine derartige Möglichkeit hin. Diese Audit stützt sich im Wesentlichen auf die im §9 des Gesetzes angesprochenen technischen und organisatorischen Maßnahmen, die in der Anlage zu diesem Paragraphen aufgeführt werden. Dieses Audit stützt sich im Wesentlichen auf die Verfahrensweise des „IT-Grundschutzhandbuches“ (leider hat es 2.000 Seiten!), das vom Bundesamt für Sicherheit in der Informationstechnik herausgegeben wird. Auf den Seiten des Bundesamtes finden sich auch Hinweise auf eine mögliche Zertifizierung.

Literatur/Links

1. http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01.htm
   Auf diesen Seiten findet sich die aktuelle Fassung des Bundesdatenschutzgesetzes
2. http://www.bsi.de/
   Die Seiten des Bundesamtes für Sicherheit in der Informationstechnik mit Download des IT-Grundschutzhandbuches.
3. http://www.johann-bizer.de/
   Die Seiten von Dr. Johann Bizer (Johann Wolfgang Goethe Universität, Frankfurt a.M., Fachbereich Rechtswissenschaft). Mit vielen Informationen zu Themen wie: e-commerce, Datenschutz, TK Datenschutz…
4. http://www.dud.de/
   Datenschutz und Datensicherheit. Betrieben vom Vieweg Verlag Wiesbaden
5. M. Böttcher, Ausgewählte Aspekte der Datensicherheit in Unternehmen
   Vortrag auf dem 23. Treffen des BME Arbeitskreises „IT-orientierte Materialwirtschaft“ (Berlin, 24.2.2004)

Autor

Prof. Dr. rer. nat. Manfred Böttcher
Technische Fachhochschule Wildau
Tel. +49 3375 508-961
mboettch@wi-bw.tfh-wildau.de