

ECC-Rechtstipp

von RA Rolf Becker (mail@rolfbecker.de)

Wenn der Hacker kommt – Rechtliche Anforderungen des Datenschutzes in Unternehmen



Datenschutzrechtliche Pflichten des Unternehmers

Datenschutz im Zusammenhang mit Facebook, Google und Co sind in aller Munde. Grund genug, sich einmal generell mit dem Datenschutz im Unternehmen zu befassen. Hier haben viele Unternehmen große und haftungsträchtige Lücken aufzuweisen.

Ein Unternehmen hortet heute, ob gewollt oder nicht, Unmengen von personenbezogenen Daten. Das beginnt mit den Daten der Arbeitnehmer und geht weiter über Kundendaten, aber auch Daten von Dienstleistern und Zulieferern. Das Recht geht davon aus, dass ein Unternehmen diese personenbezogenen Daten gegen Eingriffe schützt, z. B. auch gegen Hackerangriffe, aber auch Mitnahme durch Mitarbeiter.

Wird der Schutz nicht gewährt, etwa weil das Aufspielen neuerer Patches vergessen wird, die Firewall nicht funktioniert oder sonst Angriffe ermöglicht werden, haftet das Unternehmen auf zivilrechtliche Schadensersatzansprüche der Geschädigten. Es kann aber auch Bußgelder geben oder die eigene Bank sieht Grundanforderungen von Basel II nicht mehr als gewährleistet an.

Führungskräfte und Arbeitnehmer haften

Wenn Sie Führungskraft im Unternehmen sind, sollte Sie dies auch berühren. Geschäftsführer (auch Gesellschaftergeschäftsführer) sind ebenso wie Vorstandsmitglieder oder Aufsichtsräte persönlich zum Schadensersatz verpflichtet, wenn die Gesellschaft einen Schaden erleidet, weil den Organen eine schuldhafte Verletzung ihrer Pflichten vorgeworfen werden muss.

Natürlich haftet auch der Arbeitnehmer, z.B. der Netzwerkadministrator, wenn er schuldhaft seinen Job nicht richtig gemacht hat und dem Unternehmen Schäden entstanden sind. Datenschutzverletzungen sind hier keine Bagatelle, wie z. B. der Administrator erfahren musste, der E-Mails seiner Vorgesetzten eingesehen hatte. Zwar hatte er die technischen Rechte dazu, nicht aber die rechtliche Legitimation (Fristlose Kündigung ohne Abmahnung rechens: Arbeitsgericht Aachen, Urt. v. 16.08.2005, Az. 7 Ca 5514/04 oder Landesarbeitsgericht München, Urt. v. 08.07.2009, Az. 11 Sa 54/09).

Technische und organisatorische Maßnahmen treffen

Hat der Beitrag Ihre Aufmerksamkeit? Es gibt eine Reihe von gesetzlichen Grundlagen, die zumindest größere Unternehmen verpflichten, Überwachungssysteme einzurichten und ein Risikomanagement für das gesamte Unternehmen zu betreiben. Die Einrichtungen sind z. B. vom Abschlussprüfer zu kontrollieren.

Doch auch kleinere Unternehmen sind von den datenschutzrechtlichen Anforderungen betroffen. Das Bundesdatenschutzgesetz verlangt eine Reihe von technischen und organisatorischen Maßnahmen, die zwingend zum Datenschutz zu treffen sind. Unternehmen haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften zu gewährleisten. Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungsprinzip sind konkrete Anforderungen, die beschreiben, wie die innerbetriebliche Organisation gestaltet werden muss, um dem Datenschutz gerecht zu werden. Es geht im Kern darum nur solchen Personen den Zugriff auf Daten zu ermöglichen, die zwingend damit zu tun haben und Daten nur zu den Zwecken zu erheben und zu verarbeiten, die zuvor festgelegt wurden.

Dazu gehört, dass Sie mit jedem Dienstleister, der Zugriff auf personenbezogene Daten hat oder haben könnte, schriftliche Vereinbarungen zur Geheimhaltung treffen und wenn die Daten „verarbeitet“ werden sollen (ein sehr weiter Begriff, der nahezu alles, was man mit Daten machen kann, umfasst), dann sind schriftliche Verträge zur Auftragsdatenverarbeitung zu treffen. Das betrifft Ihren EDV-Dienstleister ebenso, wie den Logistiker, der Kundenaufträge weiter verarbeitet. Dort, wo auch nur die schriftliche Niederlegung fehlt oder in der schriftlichen Niederlegung bestimmte Festlegungen fehlen, drohen drastische Geldbußen bis zu 300.000 EUR (vgl. § 43 BDSG).

Daneben gibt es die Institution des Datenschutzbeauftragten, der als Sachwalter der Interessen der potentiell Betroffenen im Betrieb möglichst unabhängig von der Weisungsbefugnis der Geschäftsleitung arbeiten soll. Der ist verpflichtend zu bestellen, wenn in der Regel mindestens 10 Mitarbeiter ständig mit der automatisierten Datenverarbeitung beschäftigt sind. Viele Unternehmen sind hier säumig und haben gar keinen Datenschutzbeauftragten.

Wenn ein Hacker zugeschlagen hat, sind oft Kreditkartendaten betroffen. Nach § 42a BDSG müssen in solchen Fällen die Datenschutzaufsichtsbehörde und die Betroffenen informiert werden. Das Gesetz kennt umfangreiche Bußgeldvorschriften und auch einen Straftatbestand. Die Sanktionen wurden im Rahmen der letzten Novellen erhöht und Bußgelder zwischen 50.000,-- Euro und 300.000,-- Euro können abschreckende Wirkung entfalten. Daneben lassen die Gerichte zunehmend auch wettbewerbsrechtliche Ansprüche auf Unterlassung zu. Damit können Wettbewerber mit Abmahnungen vorgehen. Wenn man so will, kann es auch eine "Strafe" sein, öffentlich mögliche Betroffene über ein Datenleck zu informieren, z. B. "durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen", wie es im § 42a BDSG heisst.

Zudem fordern Kreditkarten-Provider häufig den Unternehmer auf, die Untersuchung durch ein Unternehmen zuzulassen, welches Beweise sichert, Sicherheitslücken finden und den vermeintlichen Tathergang ermitteln soll. Nach den AGB der Kartenunternehmen können zudem Vertragsstrafen von 10.000 EUR bzw. Dollar drohen.

Praxishinweis:

Die Anforderungen des Datenschutzes in Unternehmen werden leicht unterschätzt. Man sollte zumindest überlegen, ob man nicht längst einen Datenschutzbeauftragten benötigt und ob die notwendigen schriftlichen Festlegungen bei der Auftragsdatenverarbeitung stattgefunden haben. Der EDV-Verantwortliche sollte in der Lage sein, Ihnen Maßnahmen zusammenzustellen, die gegen die missbräuchliche Datenverwendung getroffen worden sind und Verbesserungsbedarf darlegen.

Zwei weitere aktuelle Rechts-Updates:**Elektronische Rechnungen jetzt leichter**

Endlich wurde am 23.09.2011 vom Bundestag (BT-Drs. 17/5125) das länger erwartete Steuervereinfachungsgesetz beschlossen. Der Bundesrat stimmte am gleichen Tag zu. Damit fällt es vor allem leichter, umsatzsteuerlich anerkannte Rechnungen auszustellen. Die bislang hohen Anforderungen fallen weg. Auch per Fax übermittelte Rechnungen reichen. Es erfolgt eine Gleichbehandlung von elektronischer Rechnung und Papierrechnung, wenn die Echtheit der Herkunft gewährleistet ist, die Rechnung unversehrt und lesbar ist und alle Pflichtangaben enthält. Eine elektronische Signatur ist nicht mehr erforderlich. Also können Rechnungen per PDF und E-Mail verschickt werden. Sie müssen allerdings weiter veränderungssicher aufbewahrt werden. Die Änderungen gelten rückwirkend am 01.07.2011.

Verbraucherrechterichtlinie angenommen

Am 10.10.2011 hat der Europäische Rat die Verbraucherrechterichtlinie, die schon am 23.06.2011 vom Parlament verabschiedet wurde, angenommen. Bestimmte Informationspflichten im Fernabsatz werden damit vollharmonisiert, gelten also im ganzen EU-Gebiet gleich.

Dazu gehören Regelungen zu Kosten der Zahlungsart, Informationen über Lieferbeschränkungen, Verbot kostenpflichtiger Kundenhotlines, Button-Lösung zur Warnung vor der Kostenpflichtigkeit des Angebots, neue Musterbelehrung, Liefertermin ist EU-weit Pflichtinformation, das Widerrufsrecht beträgt EU-weit 14 Tage. Weitere Bestimmungen sind: die Kosten der Rücksendung trägt der Verbraucher, Hinsendekosten (keine Expresszuschläge) trägt der Händler, es gibt neue Ausnahmen vom Widerrufsrecht (z. B. für „hygienisch sensible“ Waren, die entsiegelt wurden) und der Verbraucher wird verpflichtet, die Waren binnen 14 Tagen zurückzusenden verbunden mit einem Zurückbehaltungsrecht für Händler.

Damit gibt es (allerdings erst in 2 Jahren, wenn die Regelungen in nationales Recht umgesetzt worden sind), deutliche Kostenerleichterungen für Händler im Bereich der Retouren.

Über den Autor

Rechtsanwalt Rolf Becker (www.rolfbecker.de) ist Partner der Rechtsanwälte WIENKE & BECKER (www.kanzlei-wbk.de) in Köln und Autor von Fachbüchern und Fachartikeln zum Wettbewerbsrecht, Markenrecht und Vertriebsrecht insbesondere im Fernabsatz. Als Mitglied im ECC-Club kommentiert Rechtsanwalt Becker für das ECC Handel regelmäßig aktuelle Urteile zum Online-Handel und gibt Händlern praktische Tipps, wie sie mit den gesetzlichen Vorgaben umgehen sollen.

Er ist auch Autor auf den Informationsdiensten

www.Versandhandelsrecht.de,

www.fernabsatz-gesetz.de,

www.arztwerberecht.de,

www.widerrufsrecht.info und

www.Urteilsticker.de.

RA Rolf Becker auf

Twitter: <http://twitter.com/rolfbecker>

Facebook: www.facebook.com/versandhandelsrecht.de

Dieser Rechtstipp ist Teil des Informationsangebots des E-Commerce-Center Handel an der IfH Institut für Handelsforschung GmbH, Köln.

Kontakt:

E-Commerce-Center Handel

c/o IfH Institut für Handelsforschung GmbH

Dürener Str. 401 b

50858 Köln

Telefon: 0221 943607-70

Fax: 0221 943607-59

E-Mail: info@ecc-handel.de

URL: <http://www.ecc-handel.de> und <http://www.ifhkoeln.de>

Erscheinungsdatum: 27. Oktober 2011