.04 CRM-User: Aufpassen auf den Datenschutz

Roland Kissling 3|5|2005

Nicht alles, was durch CRM-Systeme möglich ist, ist rechtlich auch zulässig. Vor allem große Unternehmen mit Auslandstöchtern müssen auf die Grundregeln im Datenschutz acht geben. Rechtsanwalt und Datenschutz-Experte Rainer Knyrim verrät im Gespräch mit der COMPUTERWELT.at die gefährlichsten Fallstricke.

CW: Interessiert das Thema Datenschutz in der IT die User überhaupt?

Knyrim: Bei einem Vortrag auf der letzten CRM-Jahrestagung bin ich sowohl bei Anbietern von CRM-Systemen, als auch bei den Anwendern auf überraschend großes Interesse für dieses Thema gestoßen. Ich hatte den Eindruck, dass dieses Thema zwar allen bewusst ist, aber keiner so recht weiss, was man tatsächlich machen darf. Die großen Anbieter haben angesichts der großen technischen Möglichkeiten fast so etwas wie ein schlechtes Gewissen.

CW: Gibt es denn CRM-Systeme, die aus Sicht des Datenschutzes bedenklich sind?

Knyrim: Bis jetzt hatten wir keinen einzigen Fall, wo man Funktionalitäten eines CRM-Systems sperren musste. Aber man muss sie richtig verwenden und bei ihrer Entwicklung und Implementierung auf den rechtlichen Rahmen Rücksicht nehmen, vor allem dann, wenn Daten länderübergreifend zentral gespeichert werden.

CW: Was sind die Knackpunkte, auf die man als Anwender achten muss?

Knyrim: Grundsätzlich hat jeder Mensch ein Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten. Unternehmen dürfen – in Ausnahme zu diesem Grundrecht – nur dann Daten speichern, wenn die Daten öffentlich zugänglich oder anonym sind, eine Zustimmung des Kunden vorliegt, oder die Daten zur Auftragserfüllung notwendig sind, ZB bei einer Bestellung.

CW: Wie verhält es sich bei Data Mining / Data Warehousing, wo man Erkenntnisse aus unterschiedlichsten Daten zur Person gewinnen will?

Knyrim: Hierfür benötige ich zuerst eine Ziel- und Zweckvorgabe und in den meisten Fällen die Zustimmung des Kunden. Der oberste Gerichtshof hat eindeutig beschrieben, wie Zustimmungen auszusehen haben. Man muss angeben, welche Datenarten zu welchem Zweck an wen gehen. „Werbezwecke" reicht als Zweck nicht aus, die Maßnahmen müssen genauer beschrieben werden. Auch an wen die Daten gehen, muss im detail festgelegt sein. „Zustimmung zur Weitergabe der Daten im Billa-Konzern zur Konsumenteninformation und für Werbemaßnahmen" zum Beispiel reichte im Kundenbindungsprogramm „Friends of Merkur" seinerzeit nicht aus. Der Kunde muss immer genau wissen, welche Unternehmen die Daten zu welchem Zweck erhalten – dies gilt umso mehr bei Data Mining und Data Warehousing Die Zustimmungsklausel darf überdies nicht in den AGB versteckt werden, sondern sollte gesondert unterschrieben werden.

CW: Diese Regelung scheint ein wenig weltfremd - Unternehmen nutzen Daten ja für die unterschiedlichsten Zwecke. Was empfehlen sie als Rechtsanwalt ihren Kunden, wie man die Zustimmung des Kunden idealerweise einholt?

Knyrim: Bei einem Klienten haben wir auf eine interne Website gelinkt, auf der alle Regelungen im Detail ersichtlich waren. Bei einem anderen, einer Bank, haben wir Kunden ein Beiblatt unterschreiben lassen, dass bei Neuanträgen immer automatisch mit ausgedruckt wird, und die jeweils aktuellen Änderungen bereits enthält.

CW: Wie sieht das mit Kalt-Aquise aus, ZB bei Anrufen oder Mailings?

Knyrim: Cold Calls für Werbezwecke sind – auch im B2B Bereich – laut §107 Abs 1 Telekommunikationsgesetz (TKG) streng verboten. Dazu zählt ZB der Verkauf irgendwelcher Abos oder Produkte. E-Mails sind im B2B Bereich zulässig, wenn es die Möglichkeit des Abmeldens gibt, und die Robinson-Liste berücksichtigt wurde. Im

privaten Bereich ZB auch dann, wenn die Person schon einmal eingekauft hat und ihre E-Mail bekanntgegeben hat. Beim physischen Postversand ist die rechtliche Situation derzeit nicht eindeutig, weil es im Datenschutzgesetz keine eindeutige Regelung gibt wie dies im TKG bei E-Mails der Fall ist. Im Zweifelsfall also lieber nicht oder nur mit ausdrücklicher vorheriger Zustimmung.

CW: Dürfen Daten innerhalb eines Unternehmensverbundes weitergegeben oder gematcht werden?

Knyrim: Die Verwendung der Daten steht und fällt mit der Zieldefinition, die im Vorhinein feststehen muss. Wenn ich ZB Daten österreichischer Kunden an meine Muttergesellschaft in Deutschland sende, um von dort zentral den Versand in Österreich zu erledigen, dürfen nicht sämtliche Daten zentral eingespielt und für alle freigegeben werden, das wäre grob rechtswidrig. Es gilt wieder die Regelung: Welche Daten zu welchem Zweck, wohin und wer hat Zugriff? Ich könnte ZB in so einem Fall einen kurzen internen Dienstleister-Vertrag aufsetzen und festlegen, dass die Daten nur für den Versand übermittelt werden, nur die Marketing-Abteilung Zugriff auf bestimmte Teile dieser Daten erhält und sie anschließend wieder gelöscht werden.

CW: Wie sieht das bei Mischkonzernen aus?

Knyrim: Das Weitergeben im Konzern ist nur dann zulässig, wenn es sich um ähnliche Unternehmenszwecke handelt. Yamaha Motors dürfte ZB keine Kunden des Yamaha Hifi-Bereichs anschreiben, wenn diese dem nicht ausdrücklich zugestimmt haben. Überdies dürfen die Melde- und Genehmigungspflichten beim Datenverarbeitungsregister und bei der Datenschutzkommission nicht vergessen werden, besonders nicht bei Datentransfers über die EU-Grenzen hinaus.

CW: Gibt es Beispiele von Unternehmen, die über datenschutzrechtliche Regelungen gestolpert sind?

Knyrim: Neben dem bekannten „Friends of Merkur"-Urteil gab es 1992 auch den Fall einer Bank, welche die Kontozeilen ihrer Kunden ausgewertet hat, um Abbuchungen für Bausparer bei fremden Banken zu identifizieren. Die Kunden wurden dann angesprochen und darauf hingewiesen, dass auch die Hausbank ein solches Angebot besitze. Einen ähnlichen Fall gab es letztes Jahr in Deutschland, wo man Kontozeilen auf Ebay-Transaktionen untersuchte, um entsprechende Kunden dann auf ein Geschäftskonto

umzustellen. Besonders krass war kürzlich der Fall eines Flüssiggaslieferanten, der Vertragskunden eines Mitbewerbes anschrieb und ihnen einen Wechsel auf sein eigenes Gas feilbot. Er konnte nicht nachweisen, dass die Daten aus dem Telefonbuch stammten, im Gegenteil: Die Adressen enthielten sogar dieselben Tippfehler wie in der Datenbank des Mitbewerbers.

CW: Ist es nicht heutzutage Gang und Gebe, Daten aus dem Unternehmen in den neuen Job mitzubringen?

Knyrim: Möglicherweise, aber die Unternehmen lassen sich das - zu Recht - nicht mehr gefallen und gehen immer härter gegen Datenklau vor. Das Datenschutzgesetz sieht generell eine Maximalstrafe von 18.890 Euro vor. Bei Gewinn- oder Schädigungsabsicht sogar bis zu einem Jahr Freiheitsstrafe. Zivilrechtlich besteht zudem die Möglichkeit auf Unterlassung und Schadenersatz zu klagen, und gegen Konkurrenten eine einstweilige Verfügung beim Handelsgericht zu erwirken.

- * -