DATENSCHUTZ UND MOBILES CRM

DATEN-SPARSAMKEIT ist geboten

MOBILES CRM (Customer Relationship Management), auf Deutsch „mobiles Kundenmanagement", ist bei mobilen Außendiensten von Unternehmen im Verkauf und Servicebereich immer verbreiteter. Doch wie sieht es beim Umgang mit Kundendaten aus datenschutzrechtlicher Sicht aus?

Viele Außendienstmitarbeiter können sich ihren Arbeitsalltag ohne Smartphone mit Zugriff auf alle wichtigen Kundendaten und andere Informationsdatenbanken nicht mehr vorstellen. Nicht weniger Kunden erwarten mittlerweile auch, dass der Service außerhalb des Unternehmens den gleichen Standard erfüllt, als wenn sie direkt vor Ort wären. Fragen zur Produktverfügbarkeit oder Lieferterminen sollen sofort beantwortet werden können und eine reibungslose und schnelle Abwicklung der Geschäftsprozesse ermöglichen. Wichtige Kundeninformationen sollen sofort aktualisiert werden. Kurzum, mobiles CRM ist in einer modernen Arbeitswelt nicht mehr wegzudenken. Datenschutzrechtlich kann der Einsatz von mobilem CRM jedoch problematisch sein.

Ab wann greift der Datenschutz?

Die Datenschutzregelungen müssen beachtet werden, sobald Unternehmen Kundendaten sortieren und wieder auffindbar speichern. Das bedeutet konkret, dass die Kundendaten grundsätzlich nur erhoben und verwendet werden dürfen, wenn der Kunde dem zugestimmt hat. Eine wirksame Einwilligung setzt dabei voraus, dass der Kunde genau weiß, welche Daten gespeichert werden und zu welchem Zweck (Zweckbindungsgrundsatz). Im B2B-Bereich wird das Einverständnis zur Speicherung der Kundendaten zum Zwecke der Kontaktaufnahme vermutet.

Rechtsanwalt Christian Solmecke (40) von der Kölner Kanzlei Wilde Beuger Solmecke hat sich auf die Beratung der Onlinebranche spezialisiert. Insgesamt arbeiten in der Kanzlei 24 Anwälte. Solmecke hat in den vergangenen Jahren den Bereich Internetrecht/E-Commerce stetig ausgebaut. So betreut er zahlreiche Medienschaffende und Web-2.0-Plattformen. Er vertritt ebenfalls tausende Filesharer, die von der Musikindustrie abgemahnt worden sind.

Welche Daten dürfen erhoben werden?

Das Bundesdatenschutzgesetz (BDSG) sieht vor, dass grundsätzlich diejenigen Daten erhoben werden dürfen, die für das vorliegende Geschäftsverhältnis objektiv erforderlich sind. Es kommt demnach immer auf das Vertragsverhältnis im Einzelfall an. Allerdings müssen an dieser Stelle immer die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet werden. Dabei muss stets abgewogen werden, ob die Erhebung der Daten zu diesem bestimmten Zweck erforderlich sind oder ob nicht das Interesse des Kunden an der Nichtnutzung seiner Daten überwiegt.

Trennungsgebot

Aus dem Zweckbindungsgrundsatz im Datenschutzrecht folgt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch entsprechend getrennt verarbeitet werden müssen. Durch dieses Trennungsgebot wird gewährleistet, dass die Nutzung der Daten nie über die erteilte Einwilligung des Kunden hinausgeht. Ein Kunde mag beispielsweise seine Daten zu vertraglichen Zwecken zur Speicherung freigegeben haben, jedoch nicht zu sonstigen Werbezwecken. Möglicherweise hat der Kunde die Werbung per Post erlaubt, jedoch die Werbung per Mail und Telefon untersagt. Die Einwilligung des Kunden für Werbemaßnahmen wird zwingend vom BDSG vorausgesetzt, sodass Unternehmen sich hier keine Fehler erlauben dürfen.

Fühlen sich Kunden durch unaufgefordert zugesandte Werbung belästigt, kann es für die Unternehmen teuer werden. Daraus folgt, dass die technische Ausgestaltung von CRM-Systemen hohen Ansprüchen gerecht werden muss. Wichtig ist dabei auch, dass die Daten über das Mobiltelefon nur über eine sichere Verbindung übertragen werden. Über das mobile CRM sollten die technischen Möglichkeiten nicht einfach ohne Einverständnis des Kunden ausgeschöpft werden.

Haftung für den Verlust der Daten

Ungeachtet der technischen Voraussetzungen, die für die Einhaltung der Datenschutzvorschriften nötig ist, stellt sich unweigerlich auch die Frage, inwieweit die Mitarbeiter für einen Datenmissbrauch oder Verlust haften. Ein Mobiltelefon kann schnell vergessen oder geklaut werden. Die rechtliche Einordnung der Haftungsfrage ist umstritten. Jedoch besteht Einigkeit darin, dass der Arbeitgeber die Verantwortung dafür trägt, dass die Mitarbeiter die nötigen datenschutzrechtlichen Vorkehrungen einhalten. Dies ergibt sich zumindest aus §9 BDSG, der besagt: „Öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes,.., zu gewährleisten." Das heißt z.B., dass Arbeitgeber dafür sorgen müssen, dass ihre Mitarbeiter ihre Telefone ausreichend vor dem Zugriff Dritter schützen und beim Speichern oder Versenden von Informationen geeignete Verschlüsselungsmethoden nutzen. Schließlich muss auch geklärt werden, wie nach einer Kündigung des Mitarbeiters die gespeicherten Kundeninformationen gelöscht werden und der Zugriff auf die Datenbank des Unternehmens verhindert wird.

Schließlich sollten weder die Kunden, noch die Kinder, noch die Lebenspartner auf die gespeicherten Daten im CRM zugreifen können. Es obliegt dem Unternehmer, ein entsprechendes Verbot gegenüber den Mitarbeitern auszusprechen und diese zum Einhalten der Verbote und Sicherheitsmaßnahmen anzuhalten.

Kunden haben einen Anspruch auf Löschung ihre Daten

Die Daten des Kundenmanagements müssen stets aktualisiert werden. Personenbezogene Daten, die nicht mehr benötigt werden, müssen gelöscht werden. Die Kunden haben nach dem BDSG einen gesetzlichen Anspruch auf die Löschung ihrer Daten. Ob die Daten noch benötigt werden, hängt vom Zweck ihrer Verwendung ab.

Mobiles CRM ist aus der modernen Arbeitswelt nicht mehr wegzudenken. Unternehmen sollten sich jedoch der datenschutzrechtlichen Relevanz bewusst sein und entsprechende Vorkehrungen treffen.

CHRISTIAN SOLMECKE