UPDATEN BEI DEN DATEN

Es dürfte deutschlandweit kaum Unternehmen geben, die keine Datensätze über ihre Kunden führen, sei es elektronisch oder in Papierform. Doch nur wenige wissen, dass am 31. August 2012 eine auch für sie relevante Übergangsfrist im Bundesdatenschutzgesetz (BDSG) abläuft. Ab September unterliegen für Werbezwecke angelegte Datenbanken noch strengeren Voraussetzungen.

Das BDSG gilt für private Unternehmen, sofern diese personenbezogene Daten von Kunden erheben, verarbeiten oder nutzen. Von der Übergangsfrist betroffen sind alle Firmen, die vor dem 1. September 2009 erhobene Kundendaten zu Werbezwecken einsetzen wollen. Es sind dabei nur wenige Nutzungsvarianten denkbar, die in diesem Sinne nicht werbender Natur sind. Unter Werbung fällt nämlich ganz allgemein jede Form der Ansprache von Menschen zur Veranlassung einer Handlung. Für nach dem 1. September 2009 erhobene Kundendaten gelten die verschärften Anforderungen des BDSG bereits heute.

Fabian Ricken (l.) und Hans-Hubert Wensing

Grundsatz: Ohne Einwilligung geht gar nichts

Folge des vom Gesetzgeber präferierten sogenannten „opt-in-Verfahrens“ ist, dass die Kunden der Verarbeitung beziehungsweise Nutzung ihrer Daten zwecks Werbung grundsätzlich ausdrücklich und zwar – von wenigen Ausnahmen abgesehen – schriftlich zustimmen müssen. Dabei ist jeder Kunde zuvor nicht nur über die Tragweite seiner Einwilligung zu informieren, sondern auch auf sein Widerspruchsrecht – das so genannte „opt-out-Verfahren“ – hinsichtlich der Verarbeitung oder Nutzung seiner Daten hinzuweisen.

Drohende Konsequenzen

Verstößt ein Unternehmen gegen die neuen Vorschriften, kann es sehr schnell sehr heikel werden: Zum einen kann sich die Aufsichtsbehörde in Gestalt des Landesdatenschutzbeauftagten – zum Beispiel nach Anzeige eines Kunden oder eines Konkurrenten – einschalten. Es können Betriebsprüfungen erfolgen und Maßnahmen, wie ein Verbot der Erhebung und Nutzung einzelner Daten, verhängt werden. Zum anderen können die Unternehmen mit Bußgeldern bis zu 300.000 Euro belegt werden. In besonders krassen Fällen kann sogar eine Strafverfolgung durch die Staatsanwaltschaft in Betracht kommen. Es drohen Geldstrafe oder Freiheitsstrafe bis zu zwei Jahren. Schlussendlich drohen einem Unternehmen, das Daten rechtswidrig verarbeitet oder nutzt, neben dem öffentlichen Ansehensverlust, Unterlassungs- und Schadensersatzklagen.

Vorgaben zum Datenmanagement

Wer bis zum 1. September 2012 seine umfangreichen Hausaufgaben erledigt und für die Zukunft vorgesorgt hat, kann die Hände aber nicht in den Schoß legen. Der Gesetzgeber hält weitere Fallstricke parat. So dürfte es noch weitgehend unbekannt sein, dass auch kleinere Unternehmen unter Umständen einen Datenschutzbeauftragten bestellen müssen.

Daneben werden Kunden nicht selten ihre Einwilligung zur Verarbeitung und Nutzung ihrer Daten von der Beantwortung von Sicherheitsfragen abhängig machen. Das bedeutet, dass bereits im Vorfeld Fragen der Datensicherheit geklärt werden müssen. Stichworte sind in diesem Zusammenhang: Rechenzentrumssicherheit, Virenschutz, Verschlüsselung, regelmäßige Back-ups, exakt definierte Zugriffsrechte, Notfallmanagement.

Empfehlung

Die Änderungen zum 1. September 2012 sollten zum Anlass genommen werden, den Datenschutz im Unternehmen auf den Prüfstand zu stellen und insbesondere die vorhandenen Datenbanken in blitzsauberen Zustand zu bringen. Andernfalls kann Ungemach drohen. ■

Die Autoren Hans-H. Wensing und Fabian Ricken sind Rechtsanwälte in der Kanzlei Harnischmacher • Löer • Wensing in Münster

Harnischmacher • Löer • Wensing
Rechtsanwälte & Notare
Westfalenstraße 173a · 48165 Münster
Tel.: 02501/4492-0
info@hlw-muenster.de
www.hlw-muenster.de