Datenschutz im Kleinst-Unternehmen

von Katrin Schweer, IHK

Unternehmen, in denen weniger als zehn Personen als eine ihrer Hauptaufgaben personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen – kurz: per Computer auf Kunden-, Lieferanten- oder Mitarbeiterdaten zugreifen – müssen in der Regel keinen Datenschutzbeauftragten bestellen und kein Verfahrensverzeichnis vorhalten. Trotzdem gelten die übrigen Vorschriften des Bundesdatenschutzgesetzes (BDSG) auch für sie.

Es gibt zwei wirtschaftliche Gründe für Unternehmen, sich um Datenschutz zu kümmern: Eine Datenschutzpanne könnte zunächst den Ruf des Unternehmens in der Öffentlichkeit schädigen, im Einzelfall sogar Schadensersatzansprüche von Geschädigten nach sich ziehen. Zum anderen könnte sie die Aufsichtsbehörde, den Landesdatenschutzbeauftragten, veranlassen, das Unternehmen einer gründlichen Prüfung zu unterziehen. Diese Prüfungen kosten zumindest Zeit und Nerven, bei krassen Rechtsverstößen können sie auch mit der Verhängung von Bußgeldern bis zu maximal 50 000 Euro enden.

Das Risiko von Datenpannen oder Beschwerden Dritter über Datenschutzmängel lässt sich bereits verringern, wenn Unternehmer mit offenen Augen durch den Betrieb gehen und dabei die zwei Grundsätze des Datenschutzes berücksichtigen: Datensparsamkeit und Datensicherheit.

Datensparsamkeit

Unternehmen dürfen personenbezogene Daten nur erheben, verarbeiten oder nutzen, soweit sie die Daten zur Erfüllung gesetzlicher Pflichten brauchen oder soweit der Betroffene in genau diese Verarbeitung etc. eingewilligt hat. Pauschal formuliert: So viele Daten wie nötig, so wenig Daten wie möglich. Dazu gehört natürlich auch, dass die Daten gelöscht werden müssen, sobald sie nicht mehr benötigt werden.

Geschützte Daten: Vom BDSG geschützt sind die personenbezogenen Daten. Das sind Angaben über einen individuellen lebenden Menschen, die diesem zugeordnet werden können. Beispiele sind Name, Anschrift, Beruf, körperliche Merkmale, Vermögen, Familienverhältnisse, Kundennummern, Konsumverhalten, Konfession, Straftaten, Vertragsverpflichtungen, Durchwahlnummern und viele weitere private oder geschäftliche Daten. Im Unternehmen gibt es typischerweise drei Gruppen von personenbezogenen Daten: Mitarbeiterdaten, Kundendaten und Lieferantendaten. Für alle drei Gruppen gilt natürlich, dass das Unternehmen alle Daten speichern darf – auch ohne Einwilligung –, die es zur Erfüllung der Verträge und zur ordnungsgemäßen Buchführung braucht. Dazu gehören Namen, Adressen, Bankverbindungen, Verträge etc.

Kundendaten: Die Basisdaten der Kunden sind unproblematisch, solange sie nur zur Abwicklung der Verträge und für die Buchführung genutzt werden. Natürlich darf man auch das Kaufverhalten analysieren, um danach das eigene Leistungsangebot auszurichten. Auch Angaben zum Zahlungsverhalten sind innerhalb eines Unternehmens kein Problem. Je nach Branche können die Daten aber auch sensible Angaben enthalten, zum Beispiel über Krankheiten. Dann ist besonders sorgfältig damit umzugehen.

Sondervorschriften greifen dann, wenn das Unternehmen die Kundendaten für gezielte Werbung nutzen will. Nicht nur das Gesetz gegen den unlauteren Wettbewerb (UWG) sondern auch § 28 BDSG enthält komplizierte Spielregeln für die Direktwerbung. Per E-Mail oder Telefon darf – zumindest bei Privatkunden – nur dann geworben werden, wenn der Umworbene in diese Werbung eingewilligt hat. Hat der Kunde bei einer früheren Bestellung seine Telekommunikationsdaten „nur so“ angegeben, reicht das als Einwilligung nicht aus. Per Briefpost darf ein Unternehmen aber weiterhin seine Bestandskunden über besondere Angebote informieren, Kataloge zusenden etc, solange der Kunde der Werbung nicht widerspricht. Auf die zahlreichen Details der Regelungen kann hier aus Platzgründen nicht näher eingegangen werden.

Vorsicht, Hacker! Dabei kann Datensicherheit oft schon mit geringen Mitteln umgesetzt werden.

Mitarbeiterdaten: Auch über die Mitarbeiter dürfen natürlich alle Daten erhoben, verarbeitet oder genutzt werden, die für Zwecke des Beschäftigungsverhältnisses, inkl. Bewerbungsverfahren, erforderlich sind. Nicht erlaubt ist dagegen das umfassende Ausforschen. So dürfen etwa krankheitsbedingte Fehlzeiten zwar systematisch erfasst werden, nicht dagegen die Art der Erkrankung oder sonstige Gesundheitsdaten. Auch verlangt der Datenschutz für die Ausforschung zur Aufdeckung von Straftaten konkrete Verdachtsmomente. Videoüberwachung ist nur sehr eingeschränkt zulässig. Beim Arbeitnehmerdatenschutz sind in der nächsten Zeit Reformen zu erwarten.

Datensicherheit

Wenn Daten einmal erhoben und gespeichert sind, müssen sie so aufbewahrt werden, dass sie vor Missbrauch und vor Verarbeitungsfehlern geschützt sind. Dabei geht es um technische und organisatorische Maßnahmen der Datensicherheit, die auch von kleinen Unternehmen mit geringen Mitteln umgesetzt werden können. Ein Aspekt ist die Zugangs- und Zugriffskontrolle: Je weniger Leute Zugang zu Daten haben, desto geringer ist das Risiko, dass Daten in die falschen Hände gelangen. Geachtet werden muss z. B. darauf, dass Kunden, Lieferanten und sonstige Besucher keinen zufälligen Einblick in die Daten haben. Oft erhöht es schon die Sicherheit, wenn der Schreibtisch so ausgerichtet wird, dass Unbefugte keinen direkten Blick auf den Bildschirm haben, genauso sollte beim Verlassen des Arbeitsplatzes ein Bildschirmschoner mit Passwortschutz aktiviert werden. Gerade in Buchhaltung und Personalbüro ist darauf zu achten, dass auch die Kollegen aus anderen Abteilungen keinen unkontrollierten Zutritt haben. Unterlagen dürfen nicht offen herumliegen, Schrankschlüssel müssen auch benutzt werden. So wie die Bürotüren gegen Einbrecher verschlossen werden, muss die EDV-Anlage durch eine Firewall vor Hackern geschützt werden.

Bei der Kommunikation ist auf Diskretion zu achten, und zwar nicht nur beim Telefonieren. E-Mails sind im Netz fast so offen wie Postkarten – sensible Daten haben darin also nichts verloren, Verschlüsselung ist ratsam. Nicht zuletzt ist der Papiermüll ein gerne übersehenes Datenleck. Er sollte entweder im Haus selbst geschreddert oder professionell entsorgt werden.

Wer mehr zum Datenschutz in Unternehmen wissen möchte, findet Informationen auf den Seiten des Bundesdatenschutzbeauftragten unter www.bfdi.bund.de, sowie auf den Seiten der Datenschutzbeauftragten der Länder (z. B. **www.lfd.niedersachsen.de**).

Buchtipp

Kundendatenschutz – Leitfaden für die Praxis

Wenn Anbieter von Waren oder Dienstleistungen potenzielle Konsumenten direkt ansprechen, so gehört das zu den effizientesten Mitteln der Kundengewinnung und -bindung. Allerdings: Nicht alles, was technisch möglich ist und betriebswirtschaftlich interessant erscheint, ist auch rechtlich erlaubt. Der Leitfaden „Kundendatenschutz“ informiert praxisorientiert über rechtmäßige Maßnahmen, aber auch über unerlaubte Aktionen, über die Rechtspositionen des umworbenen Kunden und über die bestehenden Kontrollmechanismen.

Zum anderen soll der Leitfaden – und das ist das eigentliche Anliegen – solchen Unternehmen Hilfe bieten, die das Medium der Direktwerbung und Methoden des Customer Relationship Managements in ihre Vertriebsstrukturen integriert haben. So beinhaltet die Beschreibung typischer Abläufe, Fallgestaltungen und rechtlicher Probleme. Erstellt wurde es von der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) gemeinsam mit dem Zentralverband der deutschen Werbewirtschaft e.V. (ZAW) und mit Unterstützung durch den DIHK. (bö)

Verlag GDD Bonn (3. Aufl. 2011), 308 Seiten, 34,90 Euro.