Technik und Recht (24): Worauf Unternehmen achten müssen, wenn sie Daten von Mitarbeitern oder Kunden sammeln

„Die Gefahr des Missbrauchs wächst“

VDI nachrichten, Mönchengladbach, 31. 3. 06, has –

Nicht alles, was machbar ist, ist auch erlaubt. Das trifft auch auf Daten zu, die von Unternehmen gesammelt werden. Um auf der sicheren Seite zu sein, sollte vor der Erhebung personenbezogener Daten die Einwillig der Betroffenen eingeholt werden. Rechtsanwältin Kerstin Zscherpe rät Unternehmen zu einem abgestuften Vorgehen, um „rechtskonform“ zu bleiben.

Die Tore zur Zukunft sind gut gesichert: mit Kameras, die sich Gesichter merken, mit Lesegeräten, die Fingerabdrücke erkennen, durch Scanner, die Irismuster unterscheiden und Funkchips, die nicht nur den Schlüsselcode, sondern Geburtsdatum, Kontostand und Bewegungsprofil ihres Trägers speichern.

Foto (M): Bilderberg/Kulka

Immer mehr Unternehmen setzen biometrische oder kombinierte Sicherungssysteme ein, ob es nun Produkte von Bosch, Sicherheitssysteme von Siemens oder von Assa Abloy sind, deren Chipkarte nicht nur per Funk die Tür aufschließt, sondern auch an der Kantine bezahlt, die Reisekosten speichert, die Parkplatzschranke öffnet und vieles mehr.

„Die Menge der erhobenen Daten wächst und damit die Gefahr des Missbrauchs“, sagt Peter Schaar, Vorsitzender der Gruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten in seinem jüngsten Abschlussbericht. Aber längst nicht alles, was machbar ist, ist auch erlaubt.

Die erste Frage, die Unternehmen beantworten müssen, lautet daher, dürfen die Daten überhaupt erhoben werden? Die Antwort darauf gibt das Bundesdatenschutzgesetz – gegebenenfalls in Kombination mit Spezialgesetzen wie der Strafprozessordnung oder dem Telekommunikationsgesetz.

Danach steht das Erheben – ebenso wie das Verarbeiten und Nutzen – personenbezogener Daten unter einem Verbot mit so genanntem Erlaubnisvorbehalt: Es ist also grundsätzlich untersagt, es sei denn, es liegen bestimmte Voraussetzungen vor, die es ausnahmsweise doch erlauben.

Eine Variante, die eine Datenerhebung zulässig macht, ist die Einwilligung, mit der die Erlaubnis der Betroffenen eingeholt wird. „Auf diese Weise bekommen Unternehmen die Freizeichnung für ihre Eingangskontrolle per Iris-Scan, für die Datenspeicherung per Kunden-Karte und vieles mehr“, erläutert Kerstin A. Zscherpe, Datenschutzspezialistin der internationalen Kanzlei Hammonds in München.

Doch das Problem mit der Einwilligung liegt auf der Hand: Manche verweigern ihre Zustimmung oder ziehen ihre schon erteilte Einwilligung kurzfristig zurück. Der Blankoschein fürs Datensammeln stößt spätestens dort an Grenzen, wo eine Vielzahl unbekannter Personen betroffen ist, etwa in einer privaten Einkaufspassage.

Hier setzt eine zulässige Datenerfassung – z. B. in Form von Videoaufnahmen – eine Interessenabwägung voraus: Das Interesse des Unternehmens an der Datenerhebung muss gegenüber dem Persönlichkeitsrecht der betroffenen Personen überwiegen. Das kann dann der Fall sein, wenn Industriespionage oder andere Straftaten zu befürchten sind, etwa Raubüberfälle in dunklen Durchgängen.

Rechtsanwältin Zscherpe rät Firmen zu einem abgestuften Vorgehen, um rechtskonform zu bleiben. So könne z. B. die Forschungsabteilung eines Pharmaunternehmens problemlos mit Iris-Scannern oder Fingerabdrucklesern gesichert werden, die Kantine desselben Unternehmens sei dagegen nicht so schutzbedürftig, weshalb biometrische Sicherungssysteme dort rechtswidrig sein könnten. „Zum Schutz des Grundrechts auf informationelle Selbstbestimmung ist immer zu prüfen, ob nicht das gleiche Ziel mit geringeren Eingriffen in das Persönlichkeitsrecht erreichbar ist“, umschreibt der Bundesdatenschutzbeauftragte Peter Schaar das Prinzip der Verhältnismäßigkeit.

Bei der Erfassung von Daten gilt das Prinzip der Verhältnismäßigkeit. Foto: Keystone

Zusätzlich zur Verhältnismäßigkeit müssen alle Datensammler das Prinzip der Zweckbindung beachten. Dient der Sicherheitschip am Labor dazu, die Forschungsergebnisse zu sichern und zeichnet er deshalb auf, wann wer das Labor betreten hat, darf die Personalabteilung die so gewonnenen Bewegungsprofile nicht ohne weiteres dazu verwenden, um beispielsweise dem Laborleiter ein mitternächtliches Schäferstündchen mit der Assistentin nachzuweisen. „Solche „Nice-to-know-Sachen sind ohne Einwilligung der Betroffenen tabu“, sagt Zscherpe.

Mitarbeiter, die sich gegen Datenmissbrauch wehren wollen, – vorausgesetzt, sie haben ihn überhaupt mitbekommen – , können dem Unternehmen recht unangenehm werden. Ohnehin hat jeder Mitarbeiter Anspruch auf Einsicht in die über ihn gespeicherten Daten. Sein erster Ansprechpartner sind die Datenschutzbeauftragten des Unternehmens. Reagieren weder die firmeninternen Datenschützer noch die Vorgesetzten, sind die öffentlichen Datenschutzbehörden zuständig – eine pro Bundesland.

„Knöpfen diese sich die Firma vor, machen sie es meist gründlich“, weiß Zscherpe. Zudem droht negatives Presseecho für das Unternehmen. Um sich solchen Ärger zu ersparen, können Firmen, die sicherheitsrelevante Technik einsetzen, regelmäßig einen Sicherheitscheck machen lassen – etwa vom TÜV oder anderen Anbietern, wie etwa dem Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein.

EVA ENGELKEN

Die Serie wird fortgesetzt. Die bisher erschienenen Artikel unter

@ www.vdi-nachrichten.com/technikundrecht