



Daten unterwegs ins Ungewisse

Ohne organisatorische, technische und regulatorische Massnahmen kann aus dem Traum der mobilen Arbeitsfreiheit bald ein rechtlicher Albtraum werden.

VON UELI GRÜTER

Der Arbeitsnomade sitzt im Zug. Er greift drahtlos auf das Netzwerk im Büro zu und holt sich die Daten, die er für seine Arbeit unterwegs benötigt. Zwischendurch spricht er übers Handy mit seinem Kollegen im Geschäft über einen Kunden und dessen Probleme; die Mitfahrer hören gespannt zu. Dann geht er zur Toilette, lässt sein Notebook und sein Handy zurück. Der Arbeitsnomade ist sich nicht bewusst, wie viele rechtliche Stolpersteine im Weg liegen, währenddem er unbekümmert durch die Welt braust.

Datenschutz und Kundengeheimnis

Der Gau für jeden CEO ist die Schlagzeile «Laptop mit 3000 Kundenadressen im Zug spurlos verschwunden!» und führt heute in der Regel zum «vorzeitigen Abgang» des Top-Kaders,

das dafür nach Datenschutzgesetz schlussendlich verantwortlich ist. Dabei sind die rechtlichen Konsequenzen zu vernachlässigen. Das Datenschutzgesetz und seine Grundsätze sind aber die rechtliche Leitplanke, an denen der Datenschutz eines Unternehmens gemessen wird, eben auch durch die Medien. Datenschutz ist darum Chefsache und entsprechende organisatorische, technische und regulatorische Massnahmen sind «top-down» anzuordnen. Damit sie auch eingehalten werden, sind die unternehmensinternen Datenschutzregeln mit drastischen Konsequenzen für den fehlbaren Mitarbeiter zu verbinden. Alles andere hätte etwa soviel Wirkung wie ein Löwe ohne Zähne.

Nicht nur Ärzte, Rechtsanwälte und Banker unterliegen einem speziellen gesetzlichen Geheimnis. Im Rahmen seiner Sorgfaltspflicht hat jedes Unternehmen neben dem Datenschutz auch nach Vertragsrecht die Vertraulichkeit seiner Kunden zu wahren. Und der Mitarbeiter seinerseits hat eine entsprechende arbeitsrechtliche, gesetzliche Geheimhaltungspflicht, die sogar über sein Arbeitsverhältnis hinaus andauert. Wird sie verletzt, kann der Arbeitgeber gegenüber dem Mitarbeiter durchgreifen, was bis zur fristlosen Entlassung führen kann.

Mobility-Reglement

Ein eigenes «Mobility-Reglement», das den Mitarbeitern als integrierender Bestandteil des Arbeitsvertrages abgegeben wird, trägt wesentlich zur Sensibilisierung und Prävention im Bereich Datenschutz und Vertraulichkeit beim mobilen Arbeiten im Unternehmen bei. Notwendig ist jedoch auch, dass im Rahmen der Anstellung genügend darauf aufmerksam gemacht und auf die arbeitsrechtlichen Konsequenzen hingewiesen wird. Das Reglement muss Teil der Weiterbildung im Unternehmen sein. Vorab wird in einem solchen Reglement festgehalten, wer welche Daten für die Arbeit



UELI GRÜTER, LL.M., IST RECHTSANWALT IN ZÜRICH UND LUZERN UND DOZENT AN DER HOCHSCHULE LUZERN MIT SPEZIALGEBIET KOMMUNIKATIONS- UND TECHNOLOGIERECHT. ER SCHARFT MIT SEINEN REGELMÄSSIGEN BEITRÄGEN AUS THEORIE UND PRAXIS DIE RECHTLICHE SICHT AUF DIE SCHWERPUNKTTHEMEN VON INFOWEEK.

ausserhalb des Unternehmens mitnehmen darf. Dafür ist eine entsprechende Klassifizierung der Daten notwendig.

Sodann wird bestimmt, mit welcher Hardware (insbesondere Laptops, PDA, Smartphones, Handys) und Software (z.B. nur autorisierte Software) die Mitarbeiter ausserhalb des Unternehmens arbeiten dürfen. Dazu gehört auch die Regelung, ob einerseits die Hardware und Software für private Zwecke eingesetzt werden dürfen und ob andererseits private Hardware und Software für die Arbeiten für das Unternehmen verwendet werden dürfen. Dazu kommt die Regelung, mit welchen Netzwerken Dritter die Geräte verbunden werden dürfen. Die Geräte müssen ausserhalb des Unternehmens derart gesichert werden, dass auch nach einem Verlust Datenschutz und Vertraulichkeit gewährleistet werden können. Dabei darf gerade der Schutz von kleinen Geräten nicht vergessen gehen. Zur Datensicherung gehören auch die organisatorischen Massnahmen, dass Datenträger nicht falschen Personen übergeben werden. Zu beachten ist zudem, was mit den Geräten passiert, wenn sie nach dem mobilen Arbeiten ins Unternehmen zurückkommen. Wenn Hard-, Software und Daten das Unter-

IN KÜRZE

- Der Gau für jeden CEO ist es, wenn vertrauliche Kundendaten wegen fehlendem Datenschutz und entsprechendem Bewusstsein der Mitarbeiter wortwörtlich auf der Strasse landen.
- Das mobile Arbeiten im Unternehmen birgt zahlreiche rechtliche Stolpersteine. Mit einem Mobility-Reglement und einer entsprechenden Bewusstseinsbildung bei den Mitarbeitern können diese rechtlichen Stolpersteine erfolgreich umschifft werden.
- Mit diesen Mitteln lassen sich allfällige rechtliche Konsequenzen und eine Beschädigung des Rufes des Unternehmens verhindern.

nehmen verlassen, muss dies protokolliert werden. Es muss jederzeit nachvollzogen werden können, wer wann welche Hard-, Software und welche Daten aus dem Unternehmen genommen hat. Das gleiche gilt für den Rücktransfer von Hard-, Software und Daten.

Datenzugriff, Übertragung

Wenn die Mitarbeiter ausserhalb des Unternehmens arbeiten, greifen sie von ihren mobilen Geräten auf die Datenbanken des Unternehmens. Dafür muss der Zutritt geregelt werden. Das Mobility-Reglement soll festlegen, wer wem zu welchen Datenbanken Zutritt gewähren darf. Dabei sollten die Berechtigungen entsprechend dem System der Unterschriftsberechtigungen für das Unternehmen vergeben werden, also «top-down», vom Verwaltungsrat zur Geschäftsleitung und von dieser zu den einzelnen Mitarbeitern. Zu den Zutrittsregeln gehört auch das Handling der Passwörter, die mit und analog zu den Zutrittsberechtigungen vergeben werden. Da Passwörter aus Sicherheitsgründen regelmässig geändert werden sollten, muss festgelegt werden, wer wann bzw. in welchen zeitlichen Abständen neue Passwörter verteilt oder die Mitarbeiter zur Änderung ihrer Passwörter auffordert. Schlussendlich müssen die Mitarbeiter zu einer sicheren Aufbewahrung von Passwörtern verpflichtet werden.

Im Rahmen des Mobility-Reglements müssen die Mitarbeiter auf eine sichere Datenübertragung sensibilisiert und dazu verpflichtet werden. Dabei ist festzuhalten, welche Datenübertragungswege die Mitarbeiter benutzen dürfen. Dazu gehört sowohl die Datenübertragung mittels Notebook, aber auch mittels Telefon und Fax. Allenfalls sind verschiedene Übertragungswege zu wählen, je nach Klassifizierung der Daten.

Da beim mobilen Arbeiten die Hardware den geschützten Raum des Unternehmens verlässt, braucht es spezielle Anweisungen zum Schutz der Hardware. So sollte z.B. geregelt werden, in welchen Umgebungen die Hardware benutzt werden darf (z.B. nur in geschlossenen Räumen, nicht in Restaurants) und wie die Hardware beaufsichtigt werden muss (z.B. keine unbeaufsichtigten Notebooks in Sitzungspausen, keine im Auto zurücklassen). Wenn auch selbstverständlich, macht es Sinn, in einem Mobility-Reglement zu erwähnen, dass die Hardware immer passwortgesi-



Wer Daten auf Reisen schickt, braucht ein Mobility-Reglement.

chert werden muss, wenn niemand daran arbeitet.

Informationssicherheit, Compliance

Der beste Soft- und Hardwareschutz nützt nichts, wenn vertrauliche Informationen ausserhalb des Unternehmens Dritten z.B. über Einsicht in den Bildschirm des Notebooks oder bei Telefonaten in der Öffentlichkeit zugänglich gemacht werden. Die Mitarbeiter müssen im Rahmen des Mobility-Reglements auf diese Problematik sensibilisiert und zu einer entsprechenden generellen Vertraulichkeit ausserhalb des Unternehmens verpflichtet werden.

Heikle Punkte, die einer Regelung bedürfen, sind beim mobilen Arbeiten ausserhalb des Unternehmens auch die Aufbewahrung und die Entsorgung von Datenträgern, Daten und ausgedruckten Dokumenten. Es stellt sich z.B. die Frage, ob diese in einer privaten Wohnung oder einem Hotelzimmer speziell gesichert, z.B. in einem abgeschlossenen Schrank oder Safe aufbewahrt werden müssen. Vor allem kleine Datenträger wie CD und Memory Sticks und ausgedruckte Dokumente landen oft in einer Tonne vor dem Haus oder werden der Altpapiersammlung mitgegeben, anstatt sie zur Entsorgung an das Unternehmen zurückzugeben oder die Dokumente genügend zu shreddern. Ungünstig ist es auch, wenn Mitarbeiter Datenträger in guten Treuen zur Entsorgung an Recycling-Unternehmen weitergeben, ohne dass das eigene Unternehmen mit diesen Vertraulichkeitsvereinbarungen hat.

Ein Schüsselement des Mobility-Reglements ist dessen Compliance. Es muss regelmäs-

sig geprüft werden, ob das Regelwerk auch effektiv eingehalten wird, da ansonsten erst bei einem Schadenfall Mängel entdeckt werden. Dabei müssen die Leute des Compliance auch Möglichkeiten haben, Verstösse gegen das Mobility-Reglement zu ahnden bzw. ahnden zu lassen. Zur Compliance gehört z.B. auch die Auswertung von im Rahmen der Erfüllung des Mobility-Reglements erstellten Protokollen.

Das durchdachteste Regelwerk nützt nichts, wenn es veraltet ist. In diesem Fall stellt das Mobility-Reglement selbst eine Gefahr dar. Aus diesem Grund ist im Regelwerk selbst zu bestimmen, wer es in welchem Rhythmus revidiert

und den neuen technischen, organisatorischen und personellen Gegebenheiten anpasst. Bei grösseren Unternehmen ist dies wohl die Leitung der IT-Abteilung zusammen mit der Rechtsabteilung.

Awareness

Obwohl davon ausgegangen werden kann, dass bereits viele Unternehmen über entsprechende Mobility-Reglemente verfügen, zeigt der tägliche sorglose Umgang mit Kundeninformationen nicht nur beim lautstarken Telefonieren in der Öffentlichkeit, dass sich die Mitarbeiter offenbar der Problematik zu wenig bewusst sind. Awareness ist aber das A und O im Bereich Datenschutz und Vertraulichkeit. Das Mobility-Reglement trägt an sich dazu bei, wenn es den Mitarbeitern im Rahmen der Anstellung entsprechend kommuniziert wird. Ergänzt werden muss diese Massnahme aber mit einer fortwährenden Sensibilisierung im Rahmen der Weiterbildung.

Sofort handeln

Und das Wichtigste: Damit mobiles Arbeiten im Unternehmen nicht zum Stolperstein für das verantwortliche Kader wird, sollte man die guten Ratschläge der Juristen nicht auf den Sanktnimmerleins-Tag verschieben, sondern sofort handeln, bevor das eigene Unternehmen den Medien ungewollt eine tolle Schlagzeile liefert. ■

WEITERFÜHRENDE INFORMATIONEN

Buch und Links zum Datenschutz: www.kommunikationsrecht.ch
Eidg. Datenschutzbeauftragter: www.edoeb.admin.ch
IT-Grundschutz-Katalog: www.bsi.de