»Strenge Trennung von Daten auf privaten Geräten ist ein Muss«

Ob Unternehmen eine Strategie dazu haben oder nicht: »Bring Your Own Device« ist bereits Realität und sollte daher klar geregelt werden. Was dabei zu beachten ist, *beschreiben Bettina Windisch-Altieri und Franz Brandstetter.*

Der Trend, dass Mitarbeiter ihre privaten Smartphones, Tablets und Laptops beruflich verwenden, wird unter Fachleuten kontroversiell diskutiert. Die einen sehen darin eine Notwendigkeit zur Steigerung der Mobilität und Produktivität sowie zur Kosteneinsparung; die anderen fürchten Sicherheits- und Haftungsrisiken für Unternehmen und raten davon ab. Gerade bei jungen, technikaffinen Arbeitnehmern ist die Akzeptanz für »Bring Your Own Device« (BYOD) hoch oder wird beim neuen Arbeitgeber mitunter zur Bedingung für einen Jobwechsel gemacht. Erlauben oder verbieten?

Welcher ist der richtige Weg für ein Unternehmen? Tatsächlich ist mobiles Arbeiten bereits längst Realität. Jedes Unternehmen kann aber entscheiden, ob es seine Mitarbeiter mit firmeneigenen Smartphones und Tablets etc. ausstattet und die Verwendung anderer Geräte verbietet oder den Einsatz privater Geräte erlaubt. Wenn das Unternehmen keine klaren Regeln setzt, läuft es Gefahr, dass Mitarbeiter ihre Geräte eigenmächtig einsetzen und das Unternehmen massive Sicherheits- und Haftungsrisiken trägt.

Es ist Pflicht der Geschäftsführung, die IT-Sicherheit und -Integrität im Unternehmen zu gewährleisten und ein wirksames Kontrollsystem und Risikomanagement zu etablieren. Sonst haftet der Geschäftsführer dem Unternehmen sogar persönlich. Umgekehrt können Schadenersatzansprüche gegenüber Dritten (Hackern) aufgrund von Mitverschulden des Unternehmens beschränkt sein, wenn keine geeigneten Schutzmaßnahmen gegen Datenverlust und -missbrauch getroffen werden. Auch Versicherungen springen in solchen Fällen unter Umständen nicht ein.

Foto: photos.com, Windisch Law, Brandstetter

Individuelle Vereinbarungen **empfohlen**

Jedes Unternehmen sollte sich daher zunächst fragen, ob mobiles Arbeiten in der eigenen Organisation erforderlich ist und welche Mitarbeiter in welchem Ausmaß mobil auf Firmendaten zugreifen müssen. Ist diese Frage geklärt, kann das Unternehmen in IT- und BYOD-Richtlinien die Rahmenbedingungen für das mobile Arbeiten schaffen. Zu prüfen ist, ob auch der Betriebsrat einzubinden ist. Kommen private Geräte der Mitarbeiter zum Einsatz, ist zusätzlich zum Arbeitsvertrag eine individuelle Nutzungsvereinbarung mit jedem Mitarbeiter zu schließen; denn hier ist das Privateigentum des Mitarbeiters betroffen, über welches der Arbeitgeber ohne Zustimmung des Mitarbeiters nicht einseitig verfügen kann.

Regelungsbedürftig in einer Nutzungsvereinbarung ist zunächst der Einsatz von Software inklusive Antivirensoftware, Apps etc., um die Sicherheitsstandards des Unternehmens zu gewährleisten. Das Unternehmen kann bestimmte Software für den Einsatz auf mobilen Geräten freigeben. Zu beachten ist, dass nur Software und Apps für geschäftliche Zwecke zum Einsatz kommen.

Das Unternehmen hat zwar den Schutz der Unternehmensdaten vor unbefugtem Zugriff und Missbrauch durch Dritte zu gewährleisten, es darf aber umgekehrt keine private Korrespondenz und Daten des Arbeitnehmers kontrollieren, verwenden oder löschen. Eine strenge Trennung von beruflichen und privaten Daten auf privaten Geräten ist ein Muss. Daher sollten keine Unternehmensdaten lokal auf dem privaten Gerät gespeichert werden. Der sichere mobile Zugriff ist durch unterschiedliche technische Lösungen wie etwa Container- oder Terminalserverlösungen und dergleichen möglich, bei welchen der Arbeitnehmer mobil nur auf die Firmendaten aus dem Netzwerk zugreifen, die bearbeiteten Daten danach auch nur im gesicherten Bereich und nicht lokal am Gerät abspeichert. Private Daten bleiben davon unberührt. Besteht eine sichere technische Trennung von beruflichem und privatem Bereich, kann der Arbeitnehmer privat das Gerät auch in der Familie zum Internetsurfen weitergeben und der Datenschutz bleibt

Bettina Windisch-Altieri, Windisch Law: »Unternehmer darf keine private Korrespondenz des Arbeitnehmers kontrollieren, verwenden oder löschen.«

Unternehmensberater Franz Brandstetter: »Sorgsame Regelung der Verwendung privater Geräte am Arbeitsplatz grenzt Haftungsrisiko ein.«

dennoch gewahrt, wofür der Arbeitgeber verantwortlich ist. Auch die sichere Verwahrung und die Verwendung des Geräts sind zu regeln. Jedes Gerät ist durch Passwort zu schützen und sollte zum Beispiel nicht sichtbar im Auto verwahrt werden. Versicherungen können ein Thema sein.

Zu regeln ist etwa auch der Ausschluss beziehungsweise die Beschränkung der Haftung im Fall von Beschädigung, Verlust oder Diebstahl des Geräts. Rechtlich kann der Arbeitgeber sonst nämlich für Verlust oder Beschädigung des privaten Geräts haften, wenn der Schaden typischerweise mit der konkreten Arbeitsleistung verbunden ist. Judikatur besteht beispielsweise für Schäden am privaten Kraftfahrzeug. Vorkehrungen zum Löschen der Daten im Fall des Verlusts eines Geräts sind zu treffen.

Risiko **einschränkbar**

Wenn ein Unternehmen BYOD sorgsam regelt, kann es letztlich auch das Haftungsrisiko gegenüber Dritten (Kunden oder Geschäftspartner) eingrenzen, wenn aufgrund einer Sorglosigkeit seiner Mitarbeiter etwa durch eingeschleppte Viren Daten eines Kunden verloren gehen oder beschädigt werden. Dasselbe gilt, wenn Urheberrechtsverletzungen passieren, beispielsweise durch das Herunterladen urheberrechtlich geschützter Inhalte, Software oder Apps. Der Arbeitgeber haftet zunächst, wenn seine Arbeitnehmer Dritten Schaden zufügen und kann sich in der Regel bei diesen nicht regressieren; denn ein Rückgriff ist ausgeschlossen, wenn der Schaden durch eine entschuldbare Fehlleistung des Arbeitnehmers entstanden ist. Bei Fahrlässigkeit kann das Gericht den Ersatz noch herabsetzen oder bei leichter Fahrlässigkeit ganz erlassen. Das Gleiche gilt, wenn der Schaden im Unternehmen des Arbeitgebers entsteht. Im Ergebnis bleibt der Schaden also meist beim Arbeitgeber hängen und kann sogar zur persönlichen Haftung des Geschäftsführers gegenüber dem Unternehmen führen. Eine solche Haftung kann man durch geeignete Nutzungsvereinbarungen mit den Arbeitnehmern abwenden.

Fazit:

BYOD ist Realität und sollte daher im Unternehmen klar geregelt werden. Dabei sind Einzelvereinbarungen zwischen Arbeitgeber und Arbeitnehmer erforderlich, um Sicherheit von Unternehmens- und Personendaten zu gewährleisten und Haftungen gegenüber Dritten auszuschließen. Auch ein gänzliches Verbot von BYOD kann geregelt werden. Nur untätiges Dulden von BYOD schadet dem Unternehmen langfristig sicher. ❐

DIE AUTOREN

Bettina Windisch-Altieri ist selbstständige Rechtsanwältin in Wien. Sie arbeitet spezialisiert im Bereich Telekom- und IT-Recht sowie IP- und Unternehmensrecht. Sie berät in- und ausländische Unternehmen jeder Branche und Größe u.a. zu unternehmensrelevanten Rechtsfragen des mobilen Arbeitens und BYOD.

www.windischlaw.com

Franz Brandstetter ist Unternehmensberater. Er arbeitet als Unternehmensjurist und Trainer im Bereich Arbeits- und Vertragsrecht und ist auf Rechtsfragen der IT und Telekommunikation spezialisiert.

www.recht-beraten.at