Foto: Brandstetter

Autor
Franz Brandstetter
Geschäftsführer,
recht-beraten Unternehmensberatung

office@recht-beraten.at

Foto: Windisch-Altieri

Autorin
Bettina Windisch-Altieri
Rechtsanwältin für Unternehmens-,
Medien- und IT-Recht

office@windischlaw.com

BYOD erlauben und regeln – Richtlinien für die Nutzung privater Endgeräte am Arbeitsplatz

Abwarten und Tee trinken oder gar ein völliges Verbot sind die schlechtesten Strategien, die Unternehmen beim Thema Einsatz privater Endgeräte am Arbeitsplatz wählen können. Denn im einen Fall laufen die Firmen Gefahr, dass sich Mitarbeiter über das Verbot hinwegsetzen. Im anderen Fall stimmt das Unternehmen durch seine Duldung BYOD konkludent zu, was zu erheblichen Haftungsrisiken führen kann. Den Einsatz privater Geräte zu erlauben und durch Richtlinien zu regeln, ist vor diesem Hintergrund ein besserer Weg. Doch welche Art von Vereinbarung eignet sich? Und welche Punkte sollte diese unbedingt klären?

Entscheidet sich ein Unternehmen dafür, seinen Mitarbeitern den Einsatz privater Geräte für berufliche Zwecke zu ermöglichen, empfiehlt es sich, bereits im Vorfeld Richtlinien festzulegen, die die Nutzung regeln. Unternehmen mit Betriebsrat können über die Nutzung privater Endgeräte für berufliche Zwecke eine Betriebsvereinbarung nach §§ 97 Abs. 1 Z1 ArbVG abschließen. Gibt es keine Arbeitnehmervertretung, müssen sie mit den Mitarbeitern individuelle Vereinbarungen im Rahmen des Dienstvertrages oder zusätzlich dazu treffen.

Wichtig ist, dass Mitarbeiter die privaten Geräte nur dann für berufliche Zwecke einsetzen dürfen, wenn sie die Nutzungsvereinbarung des Arbeitgebers unterzeichnet haben. Für den Fall des Missbrauchs oder wenn sich der Einsatz des privaten Geräts bei einem Mitarbeiter als ungeeignet erweist, muss die Nutzungsvereinbarung von Seiten des Arbeitgebers künd- oder widerrufbar sein. Im Extremfall kann der Verstoß gegen

die Nutzungsvereinbarung auch zur Entlassung des Arbeitnehmers wegen beharrlicher Pflichtverletzung oder Vertrauensunwürdigkeit führen.

Folgende Punkte sollten Unternehmen, die BYOD erlauben, beachten und in der Nutzungsvereinbarung regeln:

Datensicherheit

Sicherheitsbestimmungen sind für BYOD-Geräte ebenso relevant wie für unternehmenseigene Geräte. Daher sollten die unternehmensinternen IT-Sicherheitsrichtlinien auch BYOD-Geräte umfassen. Grundsätzlich gilt sowohl für unternehmenseigene wie für BYOD-Geräte, dass ein Schutz vor

- Schadprogrammen und Viren,
- unbefugtem Abhören sowie
- Ausspionieren von Passwörtern

gewährleistet sein muss. Dies sollte der Arbeitgeber sicherstellen. Bevor ein Mitarbeiter ein Gerät beruflich nutzen darf, muss das Unternehmen entscheiden, welche Software, Downloads oder Apps verboten sind, welche die Mitarbeiter verwenden dürfen und welche als Voraussetzung für BYOD installiert werden müssen. Dies auch, um eine mögliche Haftung des Arbeitgebers etwa bei Verstoß gegen Lizenzbestimmungen hintanzuhalten. Darüber hinaus sollten Arbeitgeber Zugriffsregeln (nur für die Mitarbeiter) und Zugriffsschutzmaßnahmen (zum Beispiel Passwörter), für die privaten Geräte etablieren und die Beschäftigten in Trainings eingehend über die die Risiken von Datendiebstahl informieren. Die Nutzung des privaten Geräts, auf dem auch berufliche Daten sind, durch Dritte (zum Beispiel Familie und Partner) ist zu untersagen, um sicherzustellen, dass ein allfälliger Schadenersatzanspruch nicht nach Dienstnehmerhaftpflichtrecht beim Arbeitgeber hängen bleibt.

Schutz und Verfügbarkeit unternehmenseigener Daten

Um die Sicherheitsstandards für die privaten Geräte zu etablieren, müssen Arbeitgeber zunächst definieren, wie die Mitarbeiter diese beruflich nutzen sollen. Eine wesentliche Frage ist dabei, ob der Dienstnehmer lediglich auf Unternehmensdaten zugreifen können soll oder ob er auch Daten auf sein BYOD-Gerät transferieren darf. Falls Daten auf ein Endgerät des Dienstnehmers geladen werden, sollten Unternehmen geeignete Schutzmaßnahmen treffen. Folgende Fragen sind hier zu beachten:

- Besteht eine klare Trennung zwischen den Daten des Arbeitgebers und den privaten Daten des Dienstnehmers? Wie werden die Daten gesichert? Sind Vertraulichkeit und Integrität für das Unternehmen gewährleistet? Es empfiehlt sich, Produkte einzusetzen, die eine Trennung der dienstlichen von den privaten Daten durch eine „Containerisierung" ermöglichen. Das geschieht entweder durch eine „Container-App", mit der alle dienstlichen Daten in einen Container „eingesperrt" werden, oder durch die Verschlüsselung der Daten mit einem nur den „verwalteten" Apps bekannten Schlüssel.
- Ist die ständige Verfügbarkeit der geschäftlichen Daten für den Arbeitgeber gewährleistet? Der Mitarbeiter sollte zum regelmäßigen Synchronisieren und Sichern der Unternehmensdaten verpflichtet werden, sofern dies nicht durch Software ohnehin automatisch passiert. Der Zugang zu Daten ist etwa im Falle einer längeren, beispielsweise krankheitsbedingten Abwesenheit des Mitarbeiters relevant. Scheidet der Mitarbeiter aus dem Unternehmen aus, muss er verpflichtet werden, sämtliche unternehmensrelevanten Daten an den Arbeitgeber zurückzugeben oder diese zu löschen.

Datenschutz

Die Bestimmungen des Datenschutzgesetzes machen nicht an der Frage halt, wem ein Gerät gehört. Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten. Dies gilt auch für private Endgeräte, auf denen Mitarbeiter beruflich genutzte personenbezogene Daten (zum Beispiel Kundendaten) speichern. Folgende Schutzmaßnahmen sind nach dem Datenschutzgesetz auch auf BYOD-Geräten notwendig:

- Wie bei firmeneigenen Geräten müssen Unternehmen auch bei beruflich genutzten Privatgeräten die Berechtigung, auf Daten und Programme zuzugreifen, so beschränken, dass Unbefugte den Datenträger weder einsehen noch verwenden können. Außerdem sollten sie festlegen, wer berechtigt ist, die Datenverarbeitungsgeräte zu verwenden. Jedes Gerät ist durch geeignete Vorkehrungen gegen die unbefugte Inbetriebnahme abzusichern. Dies kann zum Beispiel durch Zugriffsberechtigungssysteme mit Passwortschutz und durch einen periodischen Wechsel der Passwörter geschehen.
- Das Datenschutzgesetz schreibt vor, dass Unternehmen ihre Sicherheitsvorkehrungen dokumentieren müssen. Diese Dokumentation erleichtert Kontrolle und Beweissicherung. Grundsätzlich müssen Arbeitgeber ein Schutzniveau gewährleisten, dass den Risiken und der Art der schützenden Daten angemessen ist, so dass die Methoden und Instrumente sehr variieren können.

Geheimhaltung

Verstöße gegen Geheimhaltungsvereinbarungen mit Kunden, Lieferanten oder Partnern werden häufig pönalisiert. Auch hier macht es keinen Unterschied, ob sich geheim zu haltende Informationen auf Firmen- oder BYOD-Geräten befinden. Der Schaden, der durch einen Verstoß gegen eine Geheimhaltungsvereinbarung entsteht, bleibt gemäß den Bestimmungen des Dienstnehmerhaftpflichtrechtes in der Regel zum größten Teil beim Arbeitgeber hängen. Hat nämlich ein Dienstnehmer bei der Erbringung seiner Dienstleistungen dem Dienstgeber durch ein Versehen einen Schaden zugefügt, so kann das Gericht aus Gründen der Billigkeit den Ersatz mäßigen oder, sofern der Schaden durch einen minderen Grad des Versehens zugefügt worden ist, auch ganz erlassen. Für eine entschuldbare Fehlleistung haftet der Mitarbeiter laut Dienstnehmerhaftpflichtgesetz (DHG) ohnehin nicht.

Verlust oder Diebstahl

Unternehmen sollten dafür Sorge tragen, dass die firmeneigenen Daten bei Verlust oder Diebstahl eines BYOD-Geräts nicht in fremde Hände geraten. Auf vielen Geräten können Unternehmen spezielle Apps einsetzen, um sämtliche Daten auf dem Mobilgerät zu löschen, wenn es verloren geht oder gestohlen wird. Unternehmensdaten sollten darüber hinaus auf den Geräten nur in verschlüsselter Form gespeichert werden. Bei einem Verlust des Geräts wird der Entschlüsselungs-Key un-

gültig gemacht und somit können die Inhalte nicht mehr genutzt werden. Die IT-Abteilung kann Daten zusätzlich mit einem „Ablaufdatum" versehen. Wenn in einem definierten Intervall kein Kontakt mit dem Server erfolgt, lassen sich die Informationen nicht mehr abrufen.

Entsorgung

Wenn mobile IT-Geräte weitergegeben oder entsorgt werden, müssen alle darauf gespeicherten Daten und Einstellungen gelöscht werden. Dazu eignet sich ein „Factory Reset", also das Zurücksetzen des Geräts in den Auslieferungszustand. Die Nutzungsvereinbarung sollte hier eine entsprechende Verpflichtung des Mitarbeiters vorsehen.

Support

Unternehmen sollten im Vorfeld klären, ob und in welchem Umfang sie auch für BYOD-Geräte technische Unterstützung bei Problemen anbieten können.

Kostenübernahme

Die Nutzungsvereinbarung sollte klären, ob sich der Arbeitgeber an den Anschaffungskosten, der Grundgebühr und etwaigen Nutzungsgebühren oder Flat-fees, Reparatur- und Wartungskosten beteiligt.

Haftung bei Beschädigung

Einer Regelung bedarf die Frage, ob der Arbeitgeber bei Beschädigung des BYOD-Gerätes haftet. Nach § 1014 ABGB ist diese Frage generell zu bejahen, wenn der Schaden mit der konkreten Arbeitsleistung typischerweise verbunden ist. Der Arbeitgeber muss beispielsweise Schäden aus der Benutzung des Privatwagens des Dienstnehmers ersetzen, wenn dem Dienstnehmer Aufgaben übertragen wurden, deren Erfüllung ohne Fahrzeug nicht möglich oder nicht zumutbar gewesen wären. Eine BYOD-spezifische Judikatur besteht allerdings zur Frage der Haftung bei Beschädigung nicht. Eine Ersatzregelung sollte daher festlegen, was der Arbeitgeber im Falle von Verlust, Diebstahl oder Beschädigung des BYOD-Gerätes bereit ist, zu ersetzen.

Fazit

Recht und IT bedingen sich bei der Frage, wie BYOD geregelt werden kann, gegenseitig. Je mehr technischer Schutz möglich ist, umso freizügiger kann eine Regelung über die Nutzung privater Geräte für berufliche Zwecke ausfallen und umgekehrt. Die Regeln sollten aber auch zu den Unternehmenswerten passen. Sie dürfen keine Inseln bleiben, die nur von Technikern und/oder Juristen bewohnt werden, sondern sollten für alle Mitarbeiter praktikabel sein.