Information

Bring Your Own Device (BYOD) - Der Einsatz privater Endgeräte im Unternehmen und die rechtliche Seite

Am eigenen Computer arbeitet man am Liebsten und am Effektivsten. Dies erkennen immer mehr Firmen und erlauben ihren Mitarbeitern die eigenen Endgeräte, wie Laptop, Tablet oder Smartphone, mit an den Arbeitsplatz zu nehmen. Die Einbindung dieser Geräte in den Arbeitsprozess des Unternehmens hat erhebliche Vorteile:

Ersparnis von Anschaffungskosten

So liegt auf der Hand, dass ein Unternehmen durch den Einsatz privater Geräte Anschaffungskosten sparen kann. Zudem sind diese Geräte oft leistungsfähiger, was sich direkt auf die Mitarbeiterzufriedenheit auswirken kann. Wer sein eigenes Notebook mit zur Arbeit bringt, arbeitet produktiver und kreativer. Und auch der Managementaufwand der IT Abteilung wird reduziert. Ein weiterer entscheidender Vorteil des BYOD-Trends ist der schnelle und sichere Zugriff auf Unternehmensanwendungen und –ressourcen unabhängig vom Standort und der Zeitzone des Mitarbeiters. Anders herum ist der Mitarbeiter auch für die Firma besser erreichbar. Das private Telefon ist ständig dabei – aber das berufliche Blackberry?

Risiken für die IT-Sicherheit

Doch selbstverständlich birgt ein solcher Trend auch Nachteile und Risiken. So stellt sich BYOD als eine rechtliche Grauzone heraus, in welcher Fragen der Datensicherheit und des IT-Compliance bisher nicht zufriedenstellend geklärt sind. Unklar ist beispielsweise die Frage wem die Daten auf privaten Endgeräten, beispielsweise beim Ausscheiden eines Mitarbeiters, gehören. Des Weiteren stellt schädliche Software auf dem privaten Endgerät eine Gefahr für die Unternehmensinfrastruktur dar. Die Einbindung der privaten Geräte in die bestehende Infrastruktur verursacht zudem erhöhte Kosten im Bezug auf Standardisierung, Vitalisierung und Remote Access.

Information

BYOD: Unaufhaltbarer Trend

Auch Produktionsausfälle oder –verzögerungen, die Verletzung von Geheimhaltungspflichten und auch der Versand von Viren kann eine Haftung des Unternehmens auslösen. Ein wasserdichtes Sicherheitskonzept ist somit elementare Voraussetzung für jedes Unternehmen, welches eine entsprechende Anpassung an BYOD bedarf um eine Haftung im Fall von Sicherheitsproblemen zu vermeiden.

Datenschutz und BYOD

Neben klassischen Schadensersatzansprüchen kann es bei BYOD auch im Zusammenhang mit dem Datenschutz zu Schwierigkeiten kommen. Die Tür zum Datenschutzrecht öffnet sich, zumindest in Deutschland, wenn personenbezogen Daten im Sinne des § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) im Spiel sind. Dazu zählen sowohl Daten der Kunden wie auch der Beschäftigten des Unternehmens. Somit ist jedes Unternehmen betroffen und eine „datenverarbeitende Stelle“ im Sinn des BDSG.

Technische und organisatorische Maßnahmen zur Datensicherheit

Das Bundesdatenschutzgetz schreibt in § 9 BDSG vor, dass verantwortliche Stellen im Sinne des § 3 BDSG technische und organisatorische Maßnahmen zur Datensicherheit erfüllen müssen. Dazu zählen insbesondere die Zugangskontrolle, also der Schutz vor unberechtigtem Zugriff und die Zugriffkontrolle, das heißt die Vergabe von dezidierten Zugriffrechten. Aber auch die Kontrolle der Weitergabe, der Eingabe und der Verfügbarkeit. Konkret bedeutet dies, dass die Daten, welche durch die Mitarbeiter auf den privaten Geräten gespeichert werden, sorgfältig geschützt und gesichert werden müssen. Das gelingt wohl nur durch Speicherung der Daten über zentrale Systeme, wie private Clouds.

Ein zusätzliches datenschutzrechtliches Problem ergibt sich bei den Überprüfungsrechten gegenüber Mitarbeitern. Der Zugriff auf das private Gerät bedarf immer der vorherigen Einwilligung des Mitarbeiters. Die Einwilligung in Beschäftigungsverhältnissen sind jedoch umstritten: jede Einwilligungserklärung nach § 4 a BDSG kann nur freiwillig abgegeben werden. Aber sind Erklärungen, die ein Arbeitnehmer gegenüber seinem Arbeitgeber abgibt, jemals freiwillig?

Information

Wem gehören die Daten?

Letztlich muss die Eigentumsfrage der Daten geklärt werden. Dabei gilt es sorgfältig zu unterscheiden: Denn nach § 903 S. 1 BGB kann man nur Eigentümer einer Sache sein. Und Daten werden nur dann als Sache im Sinne des § 90 BGB angesehen, wenn sie als konkretisierte Information körperlich begrenzbar sind. Liegen die konkretisierten Informationen dagegen körperlich unbegrenzt vor, sind sie keine Sachen nach dem Gesetz.

Rund um BYOD bilden sich also zahlreiche rechtliche Problemfelder die durch sog. BYOD-Richtlinien und vertraglichen Vereinbarungen mit den einzelnen Mitarbeiten in den Griff zu bekommen sind. Hierbei stellen sich einige Maßnahmen als besonders wirksam heraus. So sollte die Speicherung von Geschäftsdaten auf dem Endgerät vermieden werden, die privaten Geräte bedürfen einer sicheren Konfiguration und unsichere Software muss ausgesperrt werden.

Abschließend lässt sich feststellen, dass BYOD viele Chancen bietet, aber auch Nachteile mit sich bringt. Die rechtlichen Anforderungen sind hoch und komplex. Daher sollte ein Unternehmen genau abwägen, ob BYOD ein Modell für den eigenen Betrieb ist.

Kontakt:
RA Sascha Leyendecker
Fachanwalt für Gewerblichen Rechtsschutz
Fachanwalt für Urheber - und Medienrecht
Tel .: 0821/34660 - 031
E - Mail: moskala@jus-kanzlei.de

RAin Alma Lena Fritz, LL.M, LL.M