Nicole Beranek Zanon

# Bring your own device (BYOD) aus rechtlicher Sicht

Zitiervorschlag: Nicole Beranek Zanon, Bring your own device (BYOD) aus rechtlicher Sicht, in: Jusletter IT 12. September 2012

Jusletter IT – Die Zeitschrift für IT und Recht
ISSN 1664-848X

www.weblaw.ch

# Bring your own device (BYOD) aus rechtlicher Sicht

Autor: Nicole Beranek Zanon
Kategorie: Scientific Articles
Rechtsgebiet(e): IT Management
Region: Switzerland

*Wenn private Geräte geschäftlich genutzt werden, stellen sich einige Rechtsfragen, die in einem Arbeitsvertragszusatz geregelt werden sollten. Der Beitrag erörtert die relevanten Fragen und gibt Antworten für das Schweizer Recht.*

Zitiervorschlag: Nicole Beranek Zanon, Bring your own device (BYOD) aus rechtlicher Sicht, in: Jusletter IT 12. September 2012

## Table of Contents



# 1 Definition

[RZ 1]

Von Bring Your Own Device (hiernach BYOD) spricht man, wenn ein Mitarbeiter sein privates (mobiles) Device wie Lap Top, Smart oder Mobile Phones, Tablet-PC usw. geschäftlich nutzt, d.h. für und innerhalb der Infrastruktur des Arbeitgebers. Der Mitarbeiter erhält somit sein Arbeitsmittel nicht oder nicht ausschliesslich mehr vom Arbeitgeber. In aller Regel, weil er dies selbst so möchte.

[RZ 2]

BYOD muss zudem nicht zwingend mit einem Cloud-Dienst verknüpft werden.

# 2 Abgrenzung

[RZ 3]

Von BYOD abzugrenzen ist die Nutzung von Mobilen Devices. Unternehmenseigene Mobile Devices unter der technischen Kontrolle des Arbeitgebers während und nach Arbeitsende des Mitarbeiters werden nicht als BYOD verstanden. Das Unterscheidungskriterium ist damit das Eigentum am Gerät.

[RZ 4]

Ebenfalls kein BYOD liegt im hier verstandenen Sinne vor, wenn Dritte (Lieferanten, Berater etc.) z.B. im Rahmen eines Projektes mit dem Mobile Device, Zugriff auf die Firmeninfrastruktur erhalten. Diese loggen sich ins Firmennetz ein, legen Dokumente ab, verwenden gewisse Firmendienste und verlassen nach Projektende das Unternehmen wieder. Selbst, wenn aus technischer Sicht in erster Line ein «fremdes» Device in die Arbeitgeber-/Auftraggeber-Infrastruktur in der einen oder anderen Form einzubinden ist, sind die rechtlichen Auswirkungen je nach Vertragsbeziehung unterschiedlich: Im Gegensatz zu BYOD ist das Verhältnis zu Dritten in der Regel nicht arbeitsrechtlicher Natur. Allfällige Verpflichtungen z.B. betreffend Datenlöschung und Geheimhaltung sind deshalb in diesen Fällen in den Lieferanten- bzw. Beratervertrag aufzunehmen.

# 3 Prozess zu BYOD

[RZ 5]

Wie wird nun BYOD im Unternehmen eingeführt? Ein BYOD-Projekt unterscheidet sich in der Vorgehensweise nicht stark von anderen IT-Projekten, mit der folgenden Ausnahme: IT-Sicherheit und die rechtlichen Rahmenbedingungen sind hier Schlüsselthemen.

## 3.1 Der Prozess im Allgemeinen

[RZ 6]

Zu beginnen ist mit einer Bedürfnisevaluation. Diese soll ermitteln, was die Mitarbeitenden und das Unternehmen benötigen. Als Zweites muss das Unternehmen eine Strategie definieren, um die Eckpunkte der Nutzung von BYOD zu regeln. Diese wird im dritten Schritt umgesetzt. Nach erfolgreicher Einführung ist ein Rückblick abzuhalten, Verbesserungen vorzunehmen und ein Compliance-Prozess zu implementieren (Abb. 1).

[RZ 7]

Die rechtliche Beurteilung von BYOD ist im Rahmen der Strategie vorzunehmen.


Abb. 1: Prozess zu BYOD

## 3.2 Bedürfnisevaluation

### 3.2.1 Argumente für die Einführung von BYOD

[RZ 8]

Es gibt einige Verkaufsargumente, weshalb BYOD in einem Unternehmen eingeführt werden sollte. Ausschlaggebend dürfte aber immer das Bedürfnis der Mitarbeiter und insbesondere des mittleren und oberen Managements sein. Letztere sind nicht nur die Treiber, sondern auch Entscheider über BYOD. Dies hat seinen berechtigten Grund. Der Mitarbeiter von heute – ein Vertreter der Generation Y – möchte mit seinen gewohnten Geräten arbeiten und gleichzeitig die privaten Informationen und Daten nutzen können. Dies verschafft ihm und dem Unternehmen mehr Effizienz. BYOD fördert damit Mitarbeiterzufriedenheit und schafft dem Unternehmen einen attraktiven Employer Brand.[1]

[RZ 9]

Aus BYOD kann sich ein finanzieller Nutzen ergeben. Mit weniger eigenen Geräten, bestehen weniger Anlagekosten, der CAPEX sinkt. Der Support, d.h. OPEX, wird hingegen gegebenenfalls komplexer und damit kostenintensiver. Die Komplexität, die sich aus der Vielfalt ergibt, wirkt sich negativ auf die Verfügbarkeit aus. Damit wird Produktivität und Effizienz verschlechtert. Support-Mitarbeiter müssen mehr Know-How zu verschiedenen Geräten bereitstellen können. Dieser Komplexität kann begegnet werden, indem man den Support an einen Dienstanbieter auslagert.[2] Nur dann dürften auch die Personalkosten sinken. Damit ändert sich die Rolle des Informatikdienstes. Der Informatikdienst wird zum Enabler, statt wie bis anhin Controller.

[RZ 10]

Nebst des Vorteils für einen attraktiven Employer Brand und den finanziellen Aspekten muss BYOD selbstverständlich auch rechtlich compliant sein sowie Gewähr bieten, dass die bestehende IT-Infrastruktur, die Dienste und die Unternehmensdaten sicherheitstechnisch geschützt werden.

### 3.2.2 Die wahren Bedürfnisse

[RZ 11]

Die wahren Bedürfnisse zur Einführung von BYOD sind aber Effizienz und Produktivität. Wer möchte schon am Arbeitsplatz mit einem alten Gerät arbeiten müssen und selbst das neuste Mobile Phone in der Tasche mit sich herumtragen, das zahlreiche Vorteile bietet? Die Verbreitung von mobilen Endgeräten führt sodann zu einer Consumerization, d.h. einer Verbreitung der IT bei den privaten Anwendern, bevor diese für Geschäftszwecke verwendet werden. Mit BYOD erfüllen wir die Erwartungen der Mitarbeiter und fördern deren Effizienz und Freude an der Arbeit.

## 3.3 Strategie definieren

[RZ 12]

Sind die Bedürfnisse klar, ist eine Strategie zu definieren (Abb. 2: Beispiel der erläuterten Strategie). Dazu ist einmal zu klären, welche i) Daten und Datensammlungen[3] vorhanden sind, ii) welche Benutzergruppen es gibt (Management/Mitarbeiter/Hilfspersonen), iii) welche Zugriffsart und -berechtigung diese erhalten, iv) welche Dienste bzw. Applikationen überhaupt mobil zugreifbar sein sollen und schliesslich v) welche Geräte eingesetzt werden sollen. Die Ziff. i) – iii)

sind Inhalte einer Daten und Access Policy.[4] Dabei ist zu beachten, dass es z.B. für die öffentliche Hand Vorgaben betreffend der Klassifikation von Akten und Daten geben kann.[5] Erst wenn die Daten- und Access Policy definiert, die Dienste und Applikationen sowie Geräte identifiziert sind, kann eine rechtlich detaillierte Beurteilung und eine Sicherheitsbeurteilung erfolgen. Das Resultat sind einzelne Use Cases, die umgesetzt werden können. Es empfiehlt sich, diese Use Cases zu Beginn einzuschränken und erst mit gesammelter Erfahrung auszudehnen.

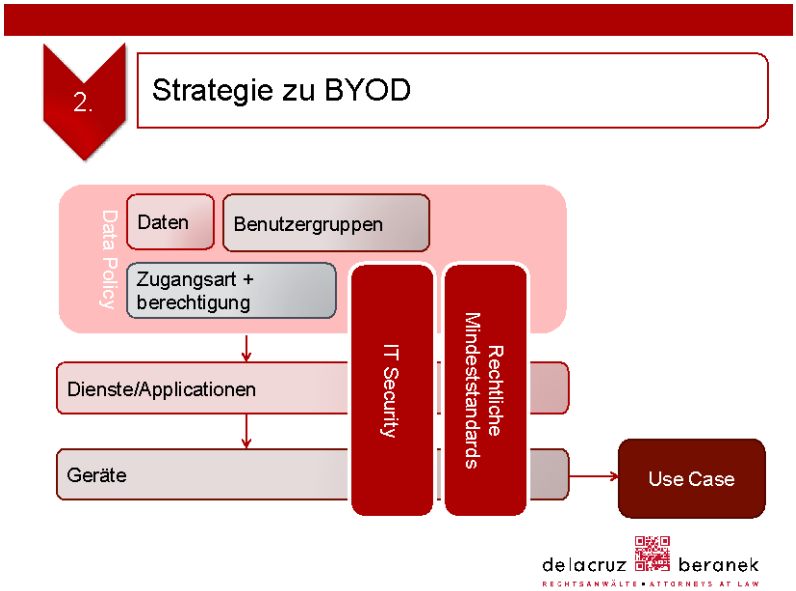


Abb. 2: Mögliche Strategie für die Implementierung von BYOD.

## 3.4 Rechtliche Beurteilung im Rahmen der BYOD-Strategie

[RZ 13]

Nachfolgend werden losgelöst von einem spezifischen Use Case die juristischen Fragestellungen und möglichen Antworten erläutert. Je nach Gerät und technischer Umsetzungen könnten sich weitere Fragen ergeben.

[RZ 14]

Im Rahmen der BYOD-Strategie sind Datenschutzfragen, arbeitsrechtliche Fragen, Fragen der Compliance, also des rechtskonformen Verhaltens, der Rechte an Immaterialgüterrechten sowie Support und Haftungsfragen zu klären. Die Antworten können dabei je nach Risikobereitschaft eines Unternehmens unterschiedlich pragmatisch oder strikt beantwortet werden.

### 3.4.1 Daten Policy

[RZ 15]

Um BYOD überhaupt rechtlich beurteilen zu können, muss erst einmal erhoben werden, was für Datenbestände im Unternehmen vorhanden sind. Anschliessend ist zu qualifizieren, ob es sich um einzelne Daten, eine Datensammlung oder eine Datensammlung im Sinne des Datenschutzgesetzes handelt.[6] Datensammlungen im Sinne des Datenschutzgesetzes sind Personendaten oder besonders schützenswerte Personendaten wie z.B. Krankheitsdaten[7]. Sodann ist ein Dateneigentümer zu bestimmen, der für die Klassifikation (z.B. öffentlich, intern, vertraulich, geheim) und der ihm zugeteilten Datenbestände verantwortlich ist. Nimmt man Qualifikation der

Daten und Klassifikation zusammen, entsteht eine Matrix die für Beurteilung, welche Daten überhaupt nicht BYOD-fähig gemacht werden dürfen, relevant ist.[8]

[RZ 16]

Bei der öffentlichen Hand sind zudem die gesetzlichen Vorgaben zur Qualifikation der Daten zu berücksichtigen.[9] Aufgrund der Klassifikation ergibt sich die Zugriffsberechtigung der verschiedenen Benutzergruppen. Sodann kann die Zugangsart festgelegt werden z.B. ob die Daten nur im Unternehmen oder auch mobil verfügbar sein sollen. Ebenfalls geregelt werden sollte, wo die Daten gespeichert werden müssen.

### 3.4.2 Arbeitsrecht

[RZ 17]

Das Verhältnis zum Mitarbeiter wird durch das Arbeitsrecht definiert. Der Arbeitsvertrag oder ein Zusatz zum Arbeitsvertrag sind deshalb die Instrumente, in denen die nachfolgenden Themen geregelt werden müssen. Wird BYOD nur im Rahmen eines Arbeitsreglements inkorporiert, ist zu prüfen, ob auf dieses im Arbeitsvertrag verwiesen wird oder ein anderer Mechanismus des Akzepts durch den Arbeitnehmer besteht.

[RZ 18]

Wird eine BYOD-Vereinbarung dem Mitarbeiter bei laufendem Arbeitsverhältnis aufgezwungen, mit dem Willen, das Arbeitsverhältnis aufrecht zu erhalten, kann je nach Inhalt eine Änderungskündigung vorliegen. Diese kann missbräuchlich sein, wenn sie sich nicht auf wirtschaftliche oder betriebliche Veränderungen abstützt.[10] Es ist deshalb vorderhand BYOD als eine Option für den Mitarbeiter einzuführen, die von sich aus BYOD wollen. BYOD kann derzeit keine Gesamtlösung für das ganze Unternehmen bis hin zum Wachmann und dem Reinigungspersonal sein.

#### 3.4.2.1 Einwilligung notwendig

[RZ 19]

Dürfen Mitarbeiter einfach ihre privaten Geräte einsetzen, um ihre Arbeitsleistung beim Arbeitgeber zu erfüllen? Nein, nach Schweizer Recht bedarf es einer Einwilligung des Arbeitgebers.[11] Diese kann auch konkludent, durch Stillschweigen und Duldung erfolgen.[12] Fehlt eine explizite Einwilligung des Arbeitgebers, besteht eine Rechtsunsicherheit. Der Mitarbeiter verletzt gegebenenfalls mit dem Einsatz von privaten Geräten seine Sorgfalts- und Treuepflicht gegenüber seinem Arbeitgeber.[13] Der Mitarbeiter ist ohne Genehmigung des Arbeitsgebers zu BYOD verpflichtet, private von geschäftlichen Daten zu trennen, gewisse Mindest-Sicherheitsstandards einzuhalten – auch wenn der Arbeitgeber diese weder definiert hat, noch dem Mitarbeiter gegeben hat.

[RZ 20]

Sind die Grundsätze der Datenaufbewahrung und –verwendung klar geregelt, kann ein Verstoss besser durch das Unternehmen belegt werden, die arbeitsrechtliche Situation ist damit klarer. Bei Verstoss einer arbeitsvertraglichen Bestimmung kommen folgende arbeitsrechtlichen Instrumente in Frage: Abmahnungen, Sperrungen des Internetzugriffs, Schadenersatzforderungen, Lohnkürzungen oder Versetzungen. Im Widerholungsfall kann eine ordentliche Kündigung ausgesprochen werden. In extremen Fällen, wie bei wiederholtem Missbrauch nach Abmahnung,

der zu technischen Störungen führt, oder bei erwiesenen Straftaten, kann der Arbeitgeber sogar die fristlose Entlassung aussprechen.[14] Eine fristlose Entlassung eines Arbeitnehmers kann einzig ausgesprochen werden, wenn dem Arbeitgeber die Fortsetzung des Arbeitsverhältnisses nach Treu und Glauben nicht mehr zugemutet werden kann (Art. 337 OR). Die Regelung über den Gebrauch von BYOD liegt daher auch im Interesse des Arbeitnehmers. Er weiss dann konkret, was in seiner Verantwortung liegt und was er vorkehren muss.

[RZ 21]

Aber auch den Interessen des Arbeitgebers dient eine schriftliche Regelung. Möchte er nämlich das private Device seines Mitarbeiters systematisch mit einem Mobile Device Management (MDM)[15] verwalten, bedarf er dazu der Einwilligung des Mitarbeiters.[16] MDM-Software sichert, überwacht, verwaltet und unterhält mobile Endgeräte unabhängig von Fernmeldedienstanbieter, Dienstleister und Firmen. MDM-Software beinhaltet die drahtlose Verteilung von Applikationen, Daten, Konfigurations-Settings und (Sicherheits-)Updates. Dies kann auch die privaten Daten, Konfigurationen und Applikationen beeinflussen. Ein Regelung für den Einsatz einer MDM-Software empfiehlt sich für Arbeitgeber nur schon deshalb, weil er die Zustimmung für ein (teilweises) Löschen – sog. Remote Wiping – auf dem Endgerät des Mitarbeiters benötigt. Dies ist relevant, wenn der Mitarbeiter das mobile Endgerät verliert oder das Arbeitsverhältnis beendet wird. Fehlt eine Einwilligung des Arbeitnehmers, verletzt der Arbeitgeber Art. 328 b OR resp. die Bestimmungen des Datenschutzgesetzes sowie das Fernmeldegeheimnis gemäss Art. 13 Abs. 1 BV[17].

[RZ 22]

Eine Löschung von Daten sollte sodann derart erfolgen, dass der Inhalt irreversibel durch Überschreiben vernichtet wird.[18] Zwar kann nicht ausgeschlossen werden, dass der ehemalige Mitarbeiter Informationen und Daten noch auf anderen als dem Arbeitgeber bekannten Geräten gespeichert hat, doch kann durch ein zertifiziertes Löschen verhindert werden, dass zumindest die bekannten Geräte der (ehemaligen) Mitarbeiter mit Informationen des Unternehmens nicht an Dritte oder Drittländer gelangen und das Unternehmen auf diese Weise böse Überraschungen in Punkto Vertraulichkeit von Kundendaten, Verletzung des Bank-, Berufs-, Amts- oder Fabrikationsgeheimnisses etc. vermeiden kann. All diese Punkte können zu massiven Imageschäden führen. Es empfiehlt sich deshalb, Mitarbeitern anzubieten, auch private Mitarbeiter-Geräte, die gegebenenfalls nie «offiziell» Firmendaten beinhaltet haben, durch die Firma zertifiziert löschen und recyceln zu lassen oder zu zerstören.

[RZ 23]

Darüber hinaus hat ein Unternehmen auch ein Interesse, dass Firmendaten zur Firma zurückgeführt werden. Mit einer MDM-Software ist dies gewährleistet. Fehlt eine solche, so sind organisatorische Prozesse zu definieren, wie und wo Firmendaten abzulegen sind (vgl. oben Daten Policy, Ziff. 3.4.1).

[RZ 24]

Ist keine MDM-Software vorhanden, muss der Mitarbeiter verpflichtet werden, den aktuellen Stand der Sicherheit einzuhalten (dazu unter Ziff. 3.4.3).

#### 3.4.2.2 Kosten

[RZ 25]

Der Arbeitgeber ist von Gesetzes wegen verpflichtet, dem Arbeitnehmer Arbeitsgeräte und -mittel zur Verfügung zu stellen. Nebst den Anschaffungskosten (Gerät, SIM-Karte und Lizenzen) betrifft dies auch die Auslagen für Abonnements-Gebühren und Internetzugang. Die Kostenübernahmepflicht gilt natürlich nur, wenn der Arbeitgeber darüber in Kenntnis gesetzt wurde und dies veranlasst resp. wissentlich geduldet hat.[19] Von dieser gesetzlich vorgesehenen Kostenübernahmepflicht kann durch spezielle Vereinbarung mit dem Mitarbeiter abgewichen werden.

#### 3.4.2.3 Klärung der Eigentumsverhältnisse

[RZ 26]

Wird ein privates Endgerät u.a. für geschäftliche Zwecke genutzt, sind die Eigentumsverhältnisse zu klären. Liegt das Eigentum beim Unternehmen, sei es durch das Zurverfügungstellung auch für private Zwecke (unter Anrechnung des Privatgebrauchs als Lohnbestandteil) oder durch einen Abkauf vom Mitarbeiter durch das Unternehmen, ermöglicht dies ein «Shared management» und den Zugriff aufs Gerät. In diesem Fall ist jedoch nicht mehr von BYOD die Rede, auch wenn der Mitarbeiter sich das Mobile Device Initial selbst beschafft hat.

[RZ 27]

Liegt das Eigentum des Mobile Devices, wie die Definition von BYOD voraussetzt, von Beginn weg beim Mitarbeiter und verbleibt es bei ihm, ist zu klären, wer Software und Apps beschafft und finanziert, mithin wem diese gehören (vgl. Dazu auch 3.4.4) und wer die Software evaluiert. Es kann Software und Apps geben, deren Verwendung dazu führt, dass Drittunternehmen Zugang zu Informationen mittels Cookies erhalten.[20]

#### 3.4.2.4 Vertragliche Regelung

[RZ 28]

Der Arbeitgeber trägt also ein erhebliches Risiko, wenn er es unterlässt, eine arbeitsvertragliche Regelung mit dem Mitarbeiter zu treffen.[21] Das Risiko lässt sich aber immerhin reduzieren. Denn der Vertragszusatz schafft beim Mitarbeiter Bewusstsein für die Problematik des Arbeitgebers.

### 3.4.3 Datenschutz, Datensicherheit und Compliance

#### 3.4.3.1 Datenschutz

[RZ 29]

Der Datenschutz ist besonders bei der Bearbeitung von Personendaten, bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen zu beachten. Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG). Dies sind im Unternehmen vorab Mitarbeiter- und Kundendaten. Seit dem Bundesgerichtsentscheid i.S. Logistep[22] können auch IP-Adressen Personendaten darstellen. Bestimmbar ist die Person nämlich dann, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist aber der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor.[23]

[RZ 30]

Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.[24]

[RZ 31]

IP-Adressen fallen bei jeglicher Art von Kommunikation (Voice-over-IP-Telefonie, SMS-Diente über Internet) an und können auch beim Surfen im Internet mit sogenannten Cookies erfasst werden. Immerhin steht fest, dass IP-Adressen im Zusammenhang mit Protokollen von HTTP-Servern Personendaten sind.[25]

[RZ 32]

Damit können viele der Daten im Unternehmen unter die Kategorie der Personendaten fallen. Personendaten dürfen nur nach den datenschutzrechtlichen Grundprinzipien bearbeitet werden:

1. Die Datenbearbeitung muss nach Treu und Glauben erfolgen und muss verhältnismässig sein. Dies bedeutet, dass die Bearbeitung von Personendaten im Rahmen von BYOD geeignet und notwendig sein muss. Unverhältnismässig ist es, wenn besonders schützenswerte Personendaten via privaten Mobile Devices von Mitarbeitern abrufbar sind. Auch hier wären Ausnahmen denkbar. Dem Mitarbeiter sollte mit BYOD nur so viel Zugriff auf Daten gegeben werden, wie er sie für seinen Tätigkeitsbereich notwendigerweise benötigt. Die Datenspeicherung auf privaten Mobile Devices statt auf dem Firmenserver muss ebenfalls verboten werden, damit das Verhältnismässigkeitsprinzip eingehalten ist.

2. Es darf nur eine rechtmässige Bearbeitung erfolgen d.h. es muss eine gesetzliche Grundlage oder ein Zustimmung des Kunden vorliegen[26].

3. Der Kunde muss der Beschaffung und dem Zweck der Datenbearbeitung zustimmen. Sie muss für ihn erkenntlich sein[27]. Es stellt sich damit im Zusammenhang mit BYOD die Frage, ob die Zustimmungsklausel der Kunden zur Datenbearbeitung nebst dem spezifischen Zweck der Personendatenbearbeitung auch einen Passus enthalten müsste, dass das Unternehmen seinen Mitarbeitern BYOD ermöglicht. Sourced ein Unternehmen die Datenbearbeitung aus, so muss die Zustimmungsklausel die Weitergabe an einen Dritten beinhalten. Analog könnte man beim BYOD argumentieren. Bei BYOD handelt es sich aber um Mitarbeiter eines Unternehmens, weshalb m.E. eine BYOD-Zustimmungsklausel vom Kunden nicht notwendig ist. Die Schlussverantwortung der Rechtmässigkeit der Datenbearbeitung obliegt immer dem Unternehmen. Es hat bei der Nutzung von BYOD durch die Mitarbeiter sicherzustellen, dass Kundendaten nicht unzulässiger Weise bearbeitet werden.

[RZ 33]

BYOD stellt damit eine besondere Herausforderung dar. Es gilt zu überwachen und zu prüfen, ob der Datenschutz eingehalten worden ist. Dies lässt sich technisch nur dann realisieren, wenn das Unternehmen Remote-Zugriff auf das Gerät des Mitarbeiters erhält.

#### 3.4.3.2 Datensicherheit

[RZ 34]

In Punkto Datensicherheit stellen sich etliche neue Anforderungen. Die Datensicherheit umfasst alle Massnahmen zur Sicherstellung der Integrität, Verfügbarkeit und Vertraulichkeit der Daten. Es müssen angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten von Daten vorgekehrt werden.[28] Insbesondere müssen unberechtigte Zugriffe von Dritten vermieden werden, indem der Zugang nach den bestehenden technischen Mitteln genützt wird. Des Weiteren sollten z.B. private Geräte nicht unbeaufsichtigt in der Öffentlichkeit liegen gelassen werden. Kleine Mobile Devices wie z.B. USB-Sticks sollten nach Gebrauch immer gelöscht und formatiert werden. Der Inhalt einer Kommunikation ist zu verschlüsseln, sobald es sich um besonders schützenswerte oder um vertrauliche Personendaten handelt (z.B. Wohnsitz und Telefonnummer einer aus dem Teilnehmerverzeichnis ausgetragenen Person). Die Mitarbeiter sind daraufhin zu schulen, dass sie in der Lage sind zu verschlüsseln. Darüber hinaus sind die Zugriffsberechtigungen durch eine Data Policy zu regeln.[29] Die Zugriffe von aussen sollten protokolliert und überwacht werden.

[RZ 35]

Die Zustimmung des Mitarbeiters für den Remote Access (bis hin zum Wiping) ist zwingend erforderlich, um datenschutzrechtskonform BYOD umzusetzen.

#### 3.4.3.3 Compliance

[RZ 36]

Nebst den sicherheitstechnischen Anforderungen sind gesetzliche und vertragliche Geheimhaltungsvorschriften zu beachten. Die Geheimhaltungsvorschriften spielen vor allem bei Geheimhaltungsvereinbarungen, M&A-Transaktionen und grösseren Forschungsprojekten eine Rolle. Geheimnisbruch kann empfindliche Konventionalstrafen[30] und strafrechtlichen Konsequenzen auslösen. Aber auch das Berufs- und Amtsgeheimnis kann verletzt werden.

[RZ 37]

Auch gesetzliche Archivierungsvorschriften für Bundesorgane oder Personen, die mit öffentlichen Aufgaben betraut sind, können sehr umfangreich sein.[31] Ohne eine zentrale Speicherung – anstelle jener auf dem Mobile Device – ist die Archivierung schlicht nicht möglich.

[RZ 38]

Zwar besteht heute keine Verpflichtung, dass Unternehmen den Fernmelde- und Internetverkehr zum Zwecke der Überwachung für die Strafermittlung ausleiten können müssen. Sie müssen aber die Ausleitung durch den Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF), der für die Strafverfolgungsbehörden die Ausleitung technisch vornimmt, ermöglichen und dulden.[32] Bei einem BYOD-Projekt ist deshalb auch kurz ein Gedanke darüber zu verlieren, wie und wo dies am einfachsten stattfinden könnte und ob das Design so gewählt werden kann, dass eine Nachrüstung problemlos ist. Technisch dürfte dies wohl beim MDM liegen.

### 3.4.4 Rechte an Immaterialgüterrechten + Lizenzrechte

[RZ 39]

Arbeitsresultate von Mitarbeitern gehören von Gesetzes wegen dem Arbeitgeber.[33] Dies gilt unabhängig davon, auf welchem Device der Mitarbeiter diese Arbeitsergebnisse erzielt hat.

[RZ 40]

Geht der Mitarbeiter noch einer Nebenbeschäftigung nach, empfiehlt es sich vorab in einem Reglement die Nebenbeschäftigung der Bewilligungspflicht des Arbeitgebers zu unterstellen. So kann sichergestellt werden, dass sämtliche Arbeitserzeugnisse dem Arbeitgeber zufallen, bzw. wenn eine Bewilligung erteilt wurde, welche Arbeitserzeugnisse in die Nebentätigkeit fallen.

[RZ 41]

Zudem ist bei BYOD die Frage der Lizenzrechte zu berücksichtigen.[34] Verwendet der Mitarbeiter auf seinen privaten Geräten geschäftliche Lizenzen, so kann dies die Lizenzrechte des Lizenzgebers verletzen und eine Klage gegen das Unternehmen auslösen (Unterlizenzierung). Es ist deshalb mit dem Mitarbeiter zu vereinbaren, in welcher Form er Lizenzen verwendet. Ebensolches ist mit dem Lizenzgeber zu prüfen, ob eine Einplatz- oder Mehrplatzlizenz für die Software besteht.[35] Ein gutes Lizenzen-Management ist dazu unabdingbar.

### 3.4.5 Support

[RZ 42]

Bei BYOD stellt sich die Frage, wie das Unternehmen dem Mitarbeiter Support bei technischen Problemen bietet. Es gibt dabei die Möglichkeit des Full-Supports, des virtuellen User-Self-Service oder gar keiner Unterstützung. Der Support kann intern oder auch extern durch einen Dienst-, Device- bzw. Lösungsanbieter erfolgen.

[RZ 43]

Es sollte nur eine begrenzte Anzahl Betriebssysteme und Software zugelassen werden. Damit lässt sich der Aufwand für den Support beschränken.[36] Beim externen Support ist mit zusätzlichen Kosten zu rechnen. Wird das Projekt von Anfang an durchkalkuliert, können die allenfalls verminderten internen Personalkosten diese Zusatzkosten im externen Support wettschlagen.[37]

### 3.4.6 Haftung

[RZ 44]

Im Zusammenhang mit BYOD gibt es einmal die bekannten Sicherheitsprobleme wie Datenleck und Intrusion (Eindringen in eine fremde Datenverarbeitungsanlage).

[RZ 45]

Zum einen kann ein mobiles Endgerät in den Besitz eines Dritten fallen, was zu Datendiebstahl, Manipulation und Angriffen auf die Gesamtinfrastruktur des Unternehmens führen kann. Besitzt ein Dritter das Endgerät nicht, kann mittels Angriff gegen die Kommunikation mit sogenannten Man-in-the-Middle-Attacken auf die Systeme des Unternehmens gegriffen werden.[38]

[RZ 46]

Weitere BYOD-spezifische Schadenspotentiale ergeben sich aufgrund der Komplexität und der erschwerten Kontrollierbarkeit der Endgeräte. Wird ein Mobile Device Management betrieben, so können die grössten technischen Risiken beschränkt werden. Dazu ist aber, wie hiervor gezeigt, die Zustimmung des Mitarbeiters notwendig. Hält sich ein Mitarbeiter nicht an die vorgegebenen Sicherheitsvorschriften, wird er haftbar.

[RZ 47]

Ohne Mobile Device Management, kann die Haftung zwar auf den Mitarbeiter abgewälzt werden. Dieser haftet, wenn er nicht sorgfältig Sicherheitsupdates installiert und die diesbezüglichen

anderen technischen Anweisungen des Arbeitgebers befolgt. Der Mitarbeiter kann sich allerdings durch den Sorgfaltsnachweis der Haftung entziehen. Dieser Beweis dürfte hingegen schwierig zu erbringen sein.[39] Ob dieser Transfer der Haftung für ein Betriebsrisiko vom Arbeitgeber zum Arbeitnehmer zulässig ist, werden wohl dereinst einmal die Gerichte entscheiden müssen. Die Haftung des Arbeitnehmers widerspricht aber grundsätzlich dem Schutzgedanken des Arbeitsrechts.

[RZ 48]

Gegenüber Dritten (Geschädigten) ist stets das Unternehmen schadenersatzpflichtig.[40] Der Arbeitgeber hat in diesem Fall ein Regressrecht gegenüber dem Mitarbeiter.

### 3.5 Konzeption, Umsetzung und Rückblick

[RZ 49]

Der Vollständigkeit halber sei noch erwähnt, dass, nachdem die Strategie definiert worden ist, die einzelnen Use Cases zu konzeptionieren sind, also mit der Umsetzung von BYOD begonnen werden kann.

[RZ 50]

Es empfiehlt sich, kleine Schritte zu machen. Wie bei jedem IT Projekt drängt sich zum Schluss auch ein Rückblick auf, um Lehren aus der Umsetzung für eine allfällige Erweiterung zu gewinnen.

## 4 Fazit

[RZ 51]

Um erfolgreich BYOD im Unternehmen einzuführen, ist eine BYOD-Strategie zu definieren. Die Hauptverantwortung liegt dabei beim Verwaltungsrat bzw. der Geschäftsleitung. Es ist der Ist-Zustand zu evaluieren, dies hinsichtlich bestehender arbeitsvertraglicher Regelungen, Weisungen und Benutzerreglemente sowie punkto Daten, Zugriffsart und -berechtigung (Daten Policy). Ergänzen Sie die Daten Policy um die Dienste und Applikationen, die notwendig sind, damit der Mitarbeiter seine Arbeit erledigen kann. Die Bearbeitung von Personendaten und besonders schützenswerte Personendaten bedürfen zusätzlicher datensicherheitstechnischer Massnahmen wie Dokumentenschutz, Verschlüsselung und sichere signierte Übertragung.

[RZ 52]

Die Eigentumsverhältnisse und die Kosten sind zu klären. Es ist dem Mitarbeiter klar zu kommunizieren, wer für Datensicherheit, Datenschutz, Lizenzen und Support verantwortlich ist, sollte kein MDM zur Anwendung kommen. Das Unternehmen muss ausserdem klare Vorgaben betreffend Back-Up und Verschlüsselung machen. Soll jederzeit sowie nach Arbeitsbeendigung ein teilweises Remote-Wiping oder ein zertifiziertes Löschen der Daten auf dem privaten Device vorgenommen werden können, so ist dies mit dem Mitarbeiter zu vereinbaren. Die Einwilligung des Unternehmens zu BYOD sollte in einem Vertragszusatz oder einem dem Mitarbeiter verbindlich zur Kenntnis gebrachten Mitarbeiterreglement festgehalten werden.

RA lic. iur. Nicole Beranek Zanon, Exec. MBA HSG, Partnerin von de la cruz beranek Rechtsanwälte AG, eine auf ICT-Recht spezialisierte Anwaltskanzlei (www.delacruzberanek.com)

[1] Barrow, Simon and Mosley, Richard, The Employer Brand, 2005, Hrsg.:Wiley, John & Sons, Incorporated; Vgl. zum Ganzen Pelkmann, Thomas, Computerwoche, 28. September 2012, abrufbar unter: http://www.computerwoche.de/netzwerke/mobile-wireless/2496315/ (Stand: 31. August 2012).
[2] Zumindest für Standardsoftware wie SAP, Microsoft etc. bestehen solche Dienste bereits.
[3] Inkl. Datensammlungen gemäss Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG, SR 235.1) mit den Kategorien Personendaten/besonders schützenswerte Personendaten.
[4] Vgl. dazu Ray, Ramon, Entrepreneur, 16. November 2011, abrufbar unter: http://www.entrepreneur.com/article/220744 (Stand: 31. August 2012).
[5] So für die Schweizerische Eidgenossenschaft: Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV, SR 510.411).
[6] Art. 4 i.V.m. 3 DSG; Bischof/Schweizer, Der Begriff der Personendaten, in: digma 2011/152, S. 153.
[7] Art. 3 lit. c DSG.
[8] Vgl. Matrix des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) im Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes in Ziff. B.9 (gemäss Art. 7 DSG), abrufbar unter http://www.edoeb.admin.ch/dokumentation/00445/00472/00935/index.html?lang=de, (Stand: 31. August 2012).
[9] Siehe FN 5; Art. 3 und 4 DSG; bspw. Art. 57h Abs. 2 RVOG (SR 172.010).
[10] BGE 123 III 246.
[11] Art. 327 Abs. 2 des Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) (SR 220).
[12] Geiser, Thomas, Aus der neueren bundesgerichtlichen Rechtsprechung zum Arbeitsrecht, in: AJP 2007, S. 1514 ff., N 2.9.
[13] Art. 321a und 321e OR.
[14] Art. 337 OR.
[15] vgl. Joseph, Abraham, Mobile Device Management - Brave New Horizon or Basic Plumbing?, abrufbar unter http://www.devicemanagement.org/content/view/20754/152/ (Stand 31. August 2012).
[16] EDÖB, Ziff. 4ff. des Leitfadens für die Bearbeitung von Personendaten im Arbeitsbereich, Bearbeitung durch private Personen, Version Mai 2011, abrufbar unter: http://www.edoeb.admin.ch/dokumentation/00445/00472/00535/index.html?lang=de (Stand: 31. August 2012).
[17] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101).
[18] Dienste für eine zertifizierte Löschung bietet z.B. InterComm AG, Cham an.
[19] Vgl. Art. 327 OR; Rehbinder/Stöckli, Berner Kommentar, Einleitung und Kommentar zu den Art. 319 – 330b OR, Band VI/2/2/1, Bern 2010, Art. 237, N 5 f.; s. z.B. auch §75 Abs. 4 Zürcher Vollzugsverordnung zum Personalgesetz (SL 177.111) betreffend Auslagenersatz für Angestellte der Universität Zürich, abrufbar unter: http://www.pa.uzh.ch/Vorgesetzte/gg1/publiclaw.html (Stand 31. August 2012).
[20] so Facebook, vgl. McMillan, Graeme, Facebook Cookies Work Even If you're Logged Out (for Your Own Good), abrufbar unter http://techland.time.com/2011/09/26/facebook-cookies-work-even-if-youre-logged-out-for-your-own-good/, (Stand 30. August 2012).
[21] Vgl. Tschol, Daniela, IT business 1/2012, «Bring your own» im Arbeitsalltag, S. 2 f., abrufbar unter: http://www.dieadvokatur.ch/fileadmin/user_upload/Publikationen/Fachartikel/2012/Bring_your_own_im_Arbeitsalltag.pdf (Stand: 31. August 2012); EDÖB Leitfaden (siehe FN 16).
[22] BGE 136 II 508.

[23] BBl 1988 II 444 f. Ziff. 221.1.
[24] BGE 136 II 508 E. 3.5 in fine.
[25] Aus BGE 136 II 508 E. 3.6 in Bezug auf Art. 2 lit. a der Richtlinie 95/46/EG (http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm unter Documents adopted/2007 [Stand: 31. August 2012]).
[26] Art. 4 Abs. 1 DSG.
[27] Art. 4 Abs. 3 und 4 DSG.
[28] Art. 7 DSG, EDÖB, Leitfaden für die Bearbeitung von Personendaten in der Bundesverwaltung, S. 9, abrufbar unter: http://www.edoeb.admin.ch/dokumentation/00445/00472/00933/index.html?lang=de, (Stand: 31. August 2012).
[29] Weber/Willi, IT-Sicherheit und Recht, in: ZIK Band Nr. 33, 2006, S. 54 ff. zu den acht Kontrollzielen nach Art. 7 Abs. 2 DSG i.V.m. Art. 9 VDSG, insbesondere zur Zugangs- und Zugriffskontrolle betreffend unbefugte Dritte; Vogt, Comuterworld.ch, 4.6.2012, abrufbar unter: http://www.computerworld.ch/marktanalysen/swissit/artikel/trend-zum-selbst-versorger-bring-your-own-device-59870/ (Stand: 31. August 2012), welcher technische Möglichkeiten zur Zugriffskontrolle erläutert, u.a. MobileIron von Swisscom.
[30] Z.B. Art. 34 und 35 DSG.
[31] Bundesgesetz vom 26. Juni 1998 über die Archivierung (Archivierungsgesetz, BGA, SR 152.1).
[32] Art. 15 Abs. 8 des Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1).
[33] Art. 332 OR und Art. 17 des Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG) (SR 231.1).
[34] Hagger Martin, Computerworld.ch, Lizenzmanagement in Zeiten von Cloud und BYOD, abrufbar unter: http://www.computerworld.ch/test/artikel/lizenzmanagement-in-zeiten-von-cloud-und-byod-60522/ (Stand: 31. August 2012).
[35] Georg Rauber, Compuersoftware, in: Urhebervertragsrecht, Zürich 2006, HRSG: Streuli-Youssef, S. 226 ff.; s. auch Clara-Ann Gordon, Handel mit Secondhand-Volumenlizenzen – auch ohne Zustimmung des Urhebers zulässig?, in: sic! 2008, S. 758 ff., welche speziell auf das Problem bei Secondhand-Volumenlizenzen eingeht.
[36] Anderson, Neil, Cisco Bring Your Own Device Device, Freedom Without Compromising the IT Network, 20.2.2012, S. 9, abrufbar unter: http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf (Stand: 31. August 2012); zum Vergleich einiger Software-Lösungen für die BYOD-Implementierung s. Swiss IT Magazine, Nr. 07/08, S. 37 ff., abrufbar unter: http://www.itmagazine.ch/heftarchiv/itm_artikel/itm_20120708_sp_marktuebersicht_BYOD.pdf (Stand: 31. August 2012).
[37] Zeitler, Rainer, ZDNet, «Bring Your Own Device»: Die Büchse der Pandora sinnvoll nutzen, 11. August 2011, abrufbar unter: http://www.zdnet.de/41555587/bring-your-own-device-die-buechse-der-pandora-sinnvoll-nutzen/ (Stand: 19. August 2012), Kostenreduktion auch durch Verwendung von Cloud-Produkten.
[38] BSI, Mobile Endgeräte und mobile Applikationen, 2006, S. 16, abrufbar unter: https://www.bsi.bund.de/ContentBSI/Publikationen/Broschueren/mobile/index_htm.html, (Stand: 31. August 2012).
[39] Art. 321a OR.
[40] Art. 55 OR.