

Bring Your Own Device – Rechtssichere Gestaltung

RA Joachim Dorschel

ITC Webinar

17.11.2011

11:00 Uhr

Zur Kanzlei

- » Bartsch Rechtsanwälte
- » Derzeit 9 Anwälte
- » Wirtschaftsrecht für Unternehmen und Unternehmer
- » National und international
- » Herausragende Kompetenz im Bereich Recht und Technik
- » Standort Karlsruhe



Zum Referenten

- » Studium in Freiburg und Tübingen
- » Tätigkeit für internationale Wirtschaftssozietät in Düsseldorf und London
- » Dissertation am Lehrstuhl Prof. Spindler zum Thema „Verträge über IT-Compliance“
- » Seit 2008 Rechtsanwalt, seit 2011 Partner bei Bartsch Rechtsanwälte
- » Beratungsschwerpunkte: IT, E-Commerce, Datenschutz, IT-Compliance, Gesellschaftsrecht für IT-Unternehmen und Investoren

Erscheinungsformen

Freie Gestaltungen

Der Arbeitgeber erlaubt die Nutzung eigener Devices außerhalb des Unternehmensnetzwerks.

Der Arbeitgeber erlaubt die Nutzung privater Devices innerhalb des Unternehmensnetzwerks.

Verpflichtende Regelungen

Der Arbeitnehmer verpflichtet sich, private Devices zu nutzen und erhält hierfür vom Arbeitgeber einen Ausgleich.

Motive

- » **Kostensenkung**
 - » Zusätzlicher Administrationsaufwand bei unzureichender Konzeption
 - » Einsparungspotenziale werden in der Praxis nicht immer realisiert

- » **Mitarbeiterbindung**
 - » Mangel an Fachkräften im IT-Bereich
 - » Alltägliche Nutzung von Smartphones
 - » Vermischung beruflicher und privater Nutzung (z. B. in Social Communities)
 - » „Selbstverständlichkeit“

Die wesentlichen rechtlichen Fragen

1. Darf der Arbeitnehmer ohne Erlaubnis des Arbeitgebers private Devices im Unternehmen nutzen?

3. Darf der Arbeitgeber erlauben, dass ein Arbeitnehmer geschützte Daten auf ein privates Device kopiert?

6. Erhöht BYOD das Haftungsrisiko des Arbeitgebers gegenüber Dritten?

2. Haftet der Arbeitgeber, wenn ein privates Device kaputt geht?

4. Wie lässt sich BYOD im Unternehmen regeln?

5. Darf ein Arbeitgeber ein privates Device kontrollieren?

7. Welche Rechte hat der Betriebsrat bei Einführung von BYOD

8. Welche Alternativen gibt es zu BYOD?

1. Darf der Arbeitnehmer ohne Erlaubnis des Arbeitgebers private Devices im Unternehmen nutzen?

BYOD ohne Zustimmung des Arbeitgebers

» **Nein**

» Rechtsfolgen

» Abmahnung und Kündigung

» Schadensersatz

» Ggf. Strafbarkeit nach § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen)

» Zumindest Schaffung einer entsprechenden Verdachtslage

» Unklare Rechtslage bei bloßer Duldung

2. Haftet der Arbeitgeber, wenn ein privates Device kaputt oder verloren geht?

Verlust und Beschädigung - Haftung des Arbeitgebers

» Sachverhalt:

Ein privates Device wird bei beschädigt oder gestohlen...

- » ...am Arbeitsplatz
- » ...auf einer Dienstreise
- » ...beim Bier in der Kneipe
- » ...aus Nachlässigkeit des Arbeitnehmers
- » ...aus Nachlässigkeit eines Kollegen
- » ...ohne, dass der Arbeitnehmer etwas dafür kann

Verlust und Beschädigung - Haftung des Arbeitgebers

- » Schutzpflicht des Arbeitgebers für berechtigterweise in den Betrieb eingebrachte Sachen des Arbeitnehmers
 - » Voraussetzung: innerer Zusammenhang mit der Arbeitsleistung
 - » Beispiele aus der Rechtsprechung: Arbeitskleidung, Privatfahrzeuge

- » Unsichere Rechtslage
 - » Uneinheitliche Einzelfallrechtsprechung
 - » Keine Entscheidungen speziell zu BYOD

Verlust und Beschädigung - Haftung des Arbeitgebers

Für und wider die Haftung des Arbeitgebers

Pro Haftung

- Nutzung auf Weisung oder mit Willen des Arbeitgebers
- Kein finanzieller Ausgleich für die Bereitstellung privater Devices
- Eigenes Verschulden des Arbeitgebers
 - Zurechnung des Verschuldens von Kollegen bei Schäden in Erfüllung von Dienstaufgaben
 - Ggf. Freistellungspflicht

Contra Haftung

- Nutzung gegen den Willen oder ohne Kenntnis des Arbeitgebers
- Finanzieller Ausgleich für die Bereitstellung privater Devices
- Mitverschulden des Arbeitnehmers
 - Arbeitnehmer-Haftungsprivileg
 - Vorsatz: Volle Haftung
 - Grobe Fahrlässigkeit: Einzelfallabwägung
 - Einfache Fahrlässigkeit: Keine Haftung

Verlust und Beschädigung - Haftung des Arbeitgebers

Zusammenfassung			
	...ohne Zustimmung des Arbeitgebers	...mit Zustimmung des Arbeitgebers ohne finanziellen Ausgleich	...mit Zustimmung des Arbeitgebers mit finanziellen Ausgleich
...am Arbeitsplatz	Haftung unwahrscheinlich	Haftung wahrscheinlich	Frage des Einzelfalls
...auf einer Dienstreise	Haftung unwahrscheinlich	Haftung wahrscheinlich	Frage des Einzelfalls
...beim Bier in der Kneipe	Haftung unwahrscheinlich	Frage des Einzelfalls	Haftung unwahrscheinlich
...aus Nachlässigkeit des Arbeitnehmers	Haftung unwahrscheinlich	Frage des Einzelfalls	Frage des Einzelfalls
...aus Nachlässigkeit eines Kollegen	Frage des Einzelfalls	Frage des Einzelfalls	Frage des Einzelfalls
...ohne, dass der Arbeitnehmer etwas dafür kann	Frage des Einzelfalls	Frage des Einzelfalls	Frage des Einzelfalls

3. Darf der Arbeitgeber erlauben,
dass ein Arbeitnehmer
geschützte Daten auf ein
privates Device kopiert?

Geschützte Daten auf privaten Devices

» Datenschutzrecht

- » Schutz personenbezogener Daten
- » Bundesdatenschutzgesetz

» Urheberrecht

- » Schutz geistiger Schöpfungen
- » Urheberrechtsgesetz

» Geheimhaltungspflichten

- » UWG und Geheimhaltungsvereinbarungen

Geschützte Daten auf privaten Devices

» Datenschutzrecht

- » Grundsatz: Eine Übermittlung personenbezogener Daten ist unzulässig, wenn sie eine Datenübermittlung (§ 3 Abs. 4 Nr. 3 BDSG) darstellt.
- » Übermitteln ist die Weitergabe von Daten an Dritte
- » Arbeitnehmer der verantwortliche Stelle sind...
 - » ...keine Dritten, wenn sie Daten im Rahmen ihrer dienstlichen Funktion erhalten
 - » ...Dritte, wenn sie Daten zu privaten oder eigenen geschäftlichen Zwecken erhalten

Geschützte Daten auf privaten Devices

» Datenschutzrecht

- » Problem: Vermischung privater und geschäftlicher Daten und Zwecke
- » Lösungsansätze:
 - » Einwilligung der Betroffenen?
 - » I.d.R. nicht praktikabel
 - » Auftragsdatenverarbeitung?
 - » Arbeitnehmer als Auftragsdatenverarbeiter?
 - » Technische Lösungen
 - » Speicherung von geschäftlichen Daten in abgeschlossenen (verschlüsselten Bereichen)
 - » Terminal-Lösungen

Geschützte Daten auf privaten Devices

» Urheberrecht

- » Installation von Software, Datenbanken o.ä., die vom Arbeitgeber unter einer Unternehmenslizenz erworben wurden, auf einem privaten Device
- » Lizenzbedingungen des Herstellers
 - » Nutzung nur auf Rechnern, die im Eigentum des Lizenznehmers stehen?
 - » AGB-rechtliche Wirksamkeit im Einzelfall prüfen
- » Rechtsunsicherheit durch fehlende Präzedenzfälle
- » Im Zweifel: Einigung mit dem Hersteller oder technische Lösung (z.B. Terminal)

Geschützte Daten auf privaten Devices

» Geheimhaltungspflichten

- » gegenüber Auftraggebern, Lieferanten, Partnern, Gesellschaftern etc.
- » Inhalt von Geheimhaltungsklauseln prüfen
 - » Speicherung von Daten nur auf Rechnern, die im Eigentum des Arbeitgebers stehen?
- » Haftung des Arbeitgebers auch für die fahrlässige Verletzung von Geheimhaltungspflichten durch den Arbeitgeber
 - » Aber: Erhöhung des Haftungsrisikos durch BYOD gegenüber betriebseigenen Mobile Devices?

4. Wie lässt sich BYOD im Unternehmen regeln ?

Regelungsmöglichkeiten

- » Direktionsrecht
 - » Problem: Privateigentum unterliegt nicht der Dispositionsbefugnis des Arbeitgebers

- » Arbeitsvertrag
 - » Detaillierte Regelung der Nutzung und Kontrolle möglich
 - » Arbeitsvertragliche Regelungen unterliegen der AGB-Kontrolle
 - » Hoher organisatorischer Aufwand in bestehenden Unternehmen
 - » Einführung und Änderung der Regelung schwierig

Regelungsmöglichkeiten

- » Betriebsvereinbarung
 - » setzt Betriebsrat voraus
 - » Weitgehende Regelungskompetenz der Verhandlungspartner
 - » Änderung der Betriebsvereinbarung wirkt automatisch auf alle Arbeitsverhältnisse

- » Die schlechteste Lösung: bloße Duldung
 - » Keine gesicherten Einfluss- und Kontrollmöglichkeiten
 - » Schwierige Änderung eines Status quo

- » Praktische Grenzen
 - » Kein Verbot der privaten Nutzung
 - » Keine Limitierung der Einsatzzwecke und Orte

5. Darf ein Arbeitgeber private Devices kontrollieren

Kontrollmöglichkeiten des Arbeitgebers

» Gesetzliche Grenzen

» § 202a StGB (Ausspähen von Daten)

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

- » Zugriff auf private Datenbestände i.d.R. nicht ausgeschlossen
- » Kein Zugriff auf private Devices unter Überwindung von Sicherheitsmechanismen des Arbeitnehmers

Kontrollmöglichkeiten des Arbeitgebers

» Gesetzliche Grenzen

- » § 32 BDSG (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses)

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

- » Kein Zugriff auf private Datenbestände außer bei konkretem Verdacht auf Straftaten
- » Rechtsunsicherheit durch Interessenabwägung

Kontrollmöglichkeiten des Arbeitgebers

» Gesetzliche Grenzen

» „Computer-Grundrecht“ des BVerfG

Das allgemeine Persönlichkeitsrecht (Art 2 Abs 1 iVm Art 1 Abs 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

- » Umfassender Schutz vor heimlicher Infiltration durch staatliche Stellen
- » Zivilrechtliche Bedeutung ungewiss (hierzu: Bartsch, CR 2008, 613 ff.)

Kontrollmöglichkeiten des Arbeitgebers

- » Rechtsfolge von Verstößen
 - » Unterlassungs- und Schadensersatzansprüche des Arbeitnehmers
 - » Beweisverwertungsverbote

- » Lösung: Einwilligung des Arbeitnehmers
 - » Schriftlich (§ 4a BDSG)
 - » Problem: AGB-Kontrolle
 - » Konkrete und enge Formulierung
 - » Rechtsunsicherheit durch fehlende Präzedenzurteile

- » Technische Trennung von dienstlichen und privaten Datenbeständen

6. Erhöht BYOD das Haftungsrisiko des Arbeitgebers gegenüber Dritten?

Haftung gegenüber Dritten

» Mögliche Haftungstatbestände

- » Vertrag
 - » Verträge über Lieferungen und Leistungen
 - » Geheimhaltungsvereinbarungen
- » Allgemeines Deliktsrecht
 - » Schutz der Integrität informationstechnischer Systeme
- » Produkthaftung
 - » Schutz der körperlichen Integrität und des Sacheigentums
 - » Verschärfung durch das Geräte- und Produktsicherheitsgesetz
- » Datenschutz
 - » Schutz personenbezogener Daten
- » Wettbewerbsrecht
 - » Schutz von Betriebsgeheimnissen
- » Urheberrecht

Haftung gegenüber Dritten

» Haftungsvermeidung

- » Reduzierung des Risikos von Schadensereignissen
- » Vermeidung eigener Haftung: Beachtung der jeweils geforderten Sorgfalt
 - » „Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt“
(§ 276 Abs. 2 BGB)
 - » Eine sichere Betriebsorganisation ist häufig entscheidend, um einen Verschuldensvorwurf zu entkräften

„Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.“

(§ 93 Abs. 1 Satz 2 AktG)

Haftung gegenüber Dritten

- » Schadens- und Haftungsszenarien auch bei mobiler Nutzung unternehmenseigener Devices
- » Schaffung einer inhomogenen IT-Landschaft durch Integration verschiedener Systeme und Standards
 - » Einheitliche Vorgaben für Hard- und Software sowie Sicherheitsstandards
 - » Regelmäßige Kontrollen
- » Grenzen der Zugriffsmöglichkeiten auf fremdes Eigentum (vgl. o.)
 - » Der Arbeitgeber begibt sich eines Teils seiner Einflussmöglichkeiten
 - » Klare Regeln im Arbeitsvertrag oder in einer Betriebsvereinbarung reduzieren das Haftungsrisiko

7. Welche Rechte hat der Betriebsrat bei Einführung von BYOD?

Mitbestimmung

Einführung von BYOD ist mitbestimmungspflichtig nach

- » § 87 Abs. 1 Nr. 1 BetrVG (Fragen der Ordnung des Betriebes und des Verhaltens der Arbeitnehmer im Betrieb)
- » § 87 Abs. 1 Nr. 6 BetrVG (Einführung und Anwendung technischer Einrichtung zur Überwachung von Verhalten und Leistung)

» Reichweite des Mitbestimmungsrechts

Das Mitbestimmungsrecht erfasst

- » jede Änderung der technischen Einrichtung (alle Änderungen, die die verarbeiteten Daten, die Programmabläufe und den Zugriffsschutz betreffen)
- » Art und Umfang der Datenverarbeitung (Welche Daten werden verarbeitet?)
- » Art und Weise der Datenverarbeitung (Wie werden die Daten verarbeitet?)
- » Durchführungsvorschriften (Regelungen über Vollzug und Kontrolle) (str.)

Rechtsfolgen der Mitbestimmungspflicht

- » Erzwingbare Mitbestimmungsrechte nach § 87 BetrVG
 - » Arbeitgeber kann Maßnahme nur einvernehmlich mit dem Betriebsrat regeln
 - » Einseitige Arbeitgeberentscheidungen sind rechtswidrig und damit unwirksam
 - » Zustimmungsverweigerung des BR ist nicht an bestimmte Gründe gebunden
 - » Initiativrecht des BR

- » Rechtsfolge
 - » Keine Durchsetzung gegen den Willen des Betriebsrates
 - » Beide Betriebsparteien können Einigungsstelle anrufen
 - » Spruch der Einigungsstelle ist bindend
 - » Unterlassungsanspruch des Betriebsrats (str.)

Schluss

Fazit

- » Kein BYOD ohne
 - » technisches Konzept und
 - » arbeitsrechtlich belastbare Regelung

- » Keine bloße ungeregelte Duldung

- » Trennung von privaten und geschäftlichen Daten
 - » Verschlüsselung
 - » Terminal-Lösungen

- » Finanzieller Ausgleich für die Nutzung

Fragen?

- » Joachim Dorschel
- » Bartsch Rechtsanwälte
- » Tel.: +49 (721) 504472 - 34
- » Fax: +49 (721) 504472 - 01
- » jd@bartsch-rechtsanwaelte.de
- » www.bartsch-rechtsanwaelte.de



Vielen Dank für Ihre Aufmerksamkeit.

- » Joachim Dorschel
- » Bartsch Rechtsanwälte
- » Tel.: +49 (721) 504472 - 34
- » Fax: +49 (721) 504472 - 01
- » jd@bartsch-rechtsanwaelte.de
- » www.bartsch-rechtsanwaelte.de

