TeleTrusT
Pioneers in IT security.

## Informationstag "IT-Sicherheit im Arbeitsrecht"

**Berlin, 15.04.2014**

# Bring Your Own Device & Derivate
# BYOD

**Matthias Hartmann / HK2 Rechtsanwälte**

HK2
Rechtsanwälte


- Rechtsanwalt
- Fachanwalt für IT-Recht
- Lehrbeauftragter der Europa-Universität Viadrina

# Einführung

- Was bedeutet BYOD
  - Bring your own device
  - Mitarbeiter nutzen eigene Geräte für die Tätigkeit im Unternehmen
    - Smartphone
    - Notebook
    - Tablet
    - Bald Google Glasses?

- Derivate
  - Consumerization of the workplace
  - Chose your own device (CYOD)
  - Mitarbeiter PC Programm (MPP) der Initiative D21

WARNING

Because of something you did,
Windows is highly unstable. You can
try to restore windows, although
that probably won't work, or restart
your stupid computer.

Choose from the following

*Press any key and get another blue screen,
probably saying that the system is critical
*Offer the computer an apology since it has
to do all your work for you
*Sacrifice something to Bill Gates and hope
he takes pity on you
*Press CTRL-ALT-DEL to restart your
computer. It won't make any difference,
you'll end up crashing it again anyway

# Positive Aspekte

- Status (Apple vs BlackBerry)
- Zufriedenheit des Mitarbeiters bei freier Wahl des Consumer-Endgerätes
- Einfache Bedienbarkeit,
- Hohe Bedienkompetenz
- Innovationsimpulse durch Nutzung aktueller Geräte
- Praktischer Nutzen durch ein Consumer-Endgerät für zwei Belange (dienstlich und privat)
- Keine Anschaffungskosten für Unternehmen
- Bessere Kommunikation mit dem Mitarbeiter bei privater Nutzung des Consumer-Endgerätes

# Probleme über Probleme

- Informationssicherheit des Unternehmens
  - Schadsoftware, Viren
  - Schutz der Betriebs- und Geschäftsgeheimnisse, § 17 UWG
  - Datenspionage durch Dritte oder den Mitarbeiter
  - Datenverlust auf privatem Gerät (Smartphone im Pool)
  - Datenverbreitung / Zufallsfunde bei Ermittlungen gegen Mitarbeiter
  - Kompromittieren der Zugangsdaten durch private Achtlosigkeit

- Datenschutz
  - Betroffene: Mitarbeiter, andere Mitarbeiter, Kunden, Dritte
  - Daten: Inhaltsdaten, Metadaten

# Probleme über Probleme

- Organisatorische Aspekte
  - Administration unterschiedlicher Geräte ohne vollen Zugriff
  - Wartung  / Reparatur
  - Verlust / Beschädigung
  - Einhaltung der Archivierungspflichten für Unternehmenskommunikation, § 257 HGB, § 147 AO
  - Einhaltung der Arbeitszeitregeln
- Software-Lizensierung
- Mitarbeiter verlässt das Unternehmen
- Steuer: (auch) private Ausgaben sind nicht abzugsfähig

# Einfach nicht beachten?

- Die Sicherheit von personenbezogenen Daten ist sicherzustellen, § 9 BDSG, § 109 Abs. 1 TKG
- Die Vertraulichkeit von Nachrichtenübermittlungssystemen ist zu gewährleisten, § 107 Abs. 2 TKG
- Das Unternehmen haftet für
  - Verletzung von Haupt- oder Nebenpflichten gegenüber Vertragspartnern, § 241 BGB (Bspw: Datenverlust durch vom MA eingeschleppten Virus)
  - bei schuldhafter Schädigung Dritter, § 823 BGB, Exkulpation für Verrichtungsgehilfen nur bei Beachtung der erforderl. Sorgfalt, § 831 BGB
  - Als Störer für kausale Beiträge an Rechtsverletzungen Dritter
  - Unterlassung bei Urheberrechtsverletzungen durch AN, § 99 UrhG
- GF haftet für Risikomanagement im Unternehmen, § 91 Abs. 2 AktG (analog)

➢ Probleme müssen angegangen werden

# Sicherheit der IT des Unternehmens

- Nutzer sind zu schulen und anzuhalten die IT-Sicherheit der Geräte zu gewährleisten
- Technische Maßnahmen sind erforderlich, um alle in der IT-Umgebung integrierten Geräte den Sicherheitsrichtlinien zu unterstellen
  - Fernzugriff auf das Gerät
  - Schreib-, Lese-, und Löschrechte
  - Fernlöschungsprogramme
  - Sichere Apps für die Arbeit installieren (Container, Virtualisierung)
  - Sicherheitsprogramme installieren (Virenscanner etc.)
  - Kontrollen durch regelmäßige Einbindung des Geräts
  - Protokollierung von Maßnahmen und Datentransfer
  - Grundrechtseingriff, also nur soweit erforderlich

- IT-Abteilung muss Risiken für alle Gerätetypen scannen und Mitarbeiter informieren über Bedrohungen

# Schutz von Daten

- Zugriff auf private Daten des Mitarbeiters ist unzulässig
- Datenverarbeitung der dienstlichen Daten unterliegt Erforderlichkeitsgrundsatz, § 32 BDSG
  - Maßnahmen der Datensicherheit ergreifen
    - Dies gilt auch für Metadaten
      - Arbeitszeiten, Aufenthaltsort, Antwortzeiten, Tätigkeit, Verhältnis zu anderen Mitarbeitern
  - Private und dienstliche Daten trennen, am besten technisch
  - Datensparsamkeit beachten
  - Vollständige Löschung von nicht mehr benötigten Daten
  - Verschlüsselung einsetzen, auch für Geräte-Backups
  - Zugriffskontrolle im Unternehmen sicherstellen
  - Umgang mit Kontrollberechtigten (DSch Aufsicht) unklar

# Finanzielle Ausgleiche

- Aufwendungsersatz für Nutzung
  - Gerätenutzung (notwendig? Bruchteil AfA?)
  - Dienstenutzung (trennbar? Pauschalen vereinbaren)
- Schäden
  - Schäden Sphäre des Nutzers
    - Gerät (Verlust, Beschädigung)
    - Daten, Programme (unwiederbringliche Katzenfotos, teure Software)
    - Verbindungskosten
    - ➢ Aufwendungsersatz, abgestuft nach Mitverschulden
  - Schäden in der Sphäre des Unternehmens
    - ➢ Innerbetrieblicher Schadensausgleich (3 Gehältergrenze?)

# Urheberrecht

- Lizenzen für die BYOD-Geräte
  - keine private Nutzung mehr, wenn dienstlich
  - Lizenzen nach Anzahl User / Concurrent User / Geräte?

  - ➢ Lizenzen des Unternehmens klären, ob beabsichtigte Nutzung zulässig und lizenziert ist
  - ➢ Mitarbeiter sensibilisieren, dass Nutzung für die Arbeit besonderer Lizenz bedürfen kann
  - ➢ Nur bestimmte Programme für die Arbeit freigeben (technisch oder organisatorisch)

- Werke des Arbeitnehmers, § 43, 69b UrhG

# Verhaltensregeln

in Arbeitssphäre

- Sparsamkeit mit Unternehmensdaten auf Device
- Kameras abkleben
- Nur Nutzung der dafür zugelassenen Programme für das Unternehmen (white list)
- Regelmäßiger Abgleich der Daten, Vertretungsfähigkeit
- Verfahren bei Beendigung
  - Kooperative Beendigung, Prozess definieren
  - unkooperative Beendigung, Risiko beim Fernzugriff: Strafbare Datenveränderung, § 303a StGB

➢ Es gelten jedenfalls die Regeln für Geräte des Unternehmens

# Verhaltensregeln

in Privatsphäre

- Sicherung vor Kenntnisnahme durch Dritte von Unternehmensdaten (keine Nutzung durch Dritte)
- Verbot der Manipulation des Gerätes (Konfigurationen, jailbreaking, rooting)
- Verbot bestimmter Programme (black list)
- Verbot bestimmter Dienste (Cloud)
- Verhalten bei Verlust
- Regelungen zur Arbeitszeit (Problem: Arbeits- / Ruhezeiten)

# Wie vereinbaren?

- Schulungen / Richtlinien / Mündliche Hinweise
  - Transparenz und Klarheit der Regeln zweifelhaft
  - Beweisprobleme
  - Kontrollverlust durch betriebliche Übung
  - Schriftliche Einwilligungen zweckmäßig, § 4 BDSG

➢ Immer beachten, es sind auch Daten Dritter betroffen, von denen keine Einwilligung vorliegt

# Wie vereinbaren

- Arbeitsvertrag / Zusatzvereinbarung (-/+)

  Schriftlich, § 4a Abs. 1 (3) BDSG (+)

  Freiwillig, § 4a Abs. 1 (1) BDSG (?)

  Aber AGB-Kontrolle, unangemessene Benachteiligungen sind unwirksam:

  Bspw: Widerrufsvorbehalte ohne sachlichen Grund; Zugriff auf private Daten, Zugriff auf Metadaten der betrieblichen Nutzung, Schadensverlagerungen

- Betriebsvereinbarung, Tarifvertrag (+)
  - Mitbestimmungspflicht nach § 87 Abs. 1 Nr. 1, 6 BetrVG
  - Keine AGB-Kontrolle (BAG 13.4.2010, 9 AZR 113/09)
  - „Andere Rechtsvorschrift“ i.S.d. § 4a BDSG
  - Aber TK-Geheimnis beachten (auch Metadaten) § 88 TKG

# Kündigungsrechte und BYOD

Ein Admin speichert unverschlüsselt Unternehmensdaten, Serverpasswörter, Zugriffsdaten, Mitarbeiterdaten auf einer privaten Festplatte zusammen mit seinen Arbeitsergebnissen, die so dem unmittelbaren Zugriff des AG entzogen sind

BAG 24.03.2011, 2 AZR 282/10: Kündigung unzulässig:

- In den betrieblichen Regeln war nur das Kopieren von Computerprogrammen untersagt, nicht das von Daten
- Es fehlte eine Weisung, wann die Arbeitsergebnisse auf die Unternehmensrechner zu überspielen gewesen wären
- Es ist nicht leichtfertig, Unternehmensdaten auf einer privaten Festplatte ungesichert abzulegen, es ist ja nichts passiert, also hätte abgemahnt werden können

HK2
Rechtsanwälte

- Generell erkennt das BAG folgende Konstellationen als kündigungsrelevant an:

  - Vireninfizierungen oder andere Störungen des betrieblichen Systems,
  - mögliche Rufschädigungen (Pornografie),
  - zusätzliche Kosten und die unberechtigte Inanspruchnahme von Betriebsmitteln;
  - die private Nutzung während der Arbeitszeit.

# Heimliche Überwachungsmaßnahmen

- BYOD ermöglicht heimliche (unzulässige) Kontrollmaßnahmen
- Verwertungsverbote wegen Verstoß gegen BDSG?
  - Nein, wenn Sozialsphäre: BAG 21.06.2012,– 2 AZR 153/11: heimliche Videoaufzeichnung öffentlicher Verkaufsfläche
  - Ja, wenn Privatsphäre: BAG 20.06.2013, 2 AZR 546/12 heimliche Schrankkontrolle
  - ➢ BYOD meist Privatsphäre betroffen

- § 32 Abs. 1 (2) BDSG Erhebung von Daten zur Aufdeckung von Straftaten

➢ Unzulässige Kontrollmaßnahmen sind u.U. strafbar nach BDSG, TKG und § 202a StGB