Bring Your Own Device (BYOD) – Der betriebliche Einsatz von Arbeitnehmereigentum

10.11.2020

Im Zeitalter der „Arbeit 4.0“ wird Arbeit vielseitiger und flexibler. Immer häufiger kommt es dazu, dass Arbeitnehmer ihr Eigentum für betriebliche Belange nutzen. Ein Beispiel ist der Einsatz eigener IT im „*Home Office*“. Diese Thematik wird arbeitsrechtlich diskutiert unter der Bezeichnung „*Bring Your Own Device*“. Die wesentlichen Aspekte, die bei „*BYOD*“ zu beachten sind, werden nachfolgend dargestellt.

1. Vorteile von „BYOD“

Als BYOD wird der Einsatz privater Endgeräte zu betrieblichen Zwecken bezeichnet. Beispiele sind betrieblich genutzte Handys, Smartphones, Tablets, Laptops u.s.w.. Das hat oftmals Vorteile für beide Seiten: Der Arbeitgeber spart Hardwarekosten und erreicht eine bessere Mitarbeitererreichbarkeit und -produktivität durch die Nutzung eines dem Arbeitnehmer vertrauten Systems. Der Arbeitnehmer muss nicht zwei Geräte verwenden und freut sich ggf., wenn der Arbeitgeber moderne private Hardware mitfinanziert.

Merke: „*BYOD*“ kann Vorteile für Arbeitgeber und Arbeitnehmer bringen.

2. Was ist bei der Einführung von BYOD zu bedenken?

Bei der Einführung von BYOD sind diverse arbeitsrechtliche Aspekte zu beachten, die nachfolgend zusammengefasst werden.

Zunächst ist zu beachten, dass BYOD **vertraglich vereinbart** werden muss. Der Arbeitgeber kann nicht im Wege des Direktionsrechts (§ 106 GewO) anordnen, dass Arbeitnehmer eigenes Equipment einsetzen. Durch eine Betriebsvereinbarung kann die Pflicht zum BYOD zu Lasten von Arbeitnehmern nicht vereinbart werden.[1]

Zu regeln ist dabei jedenfalls die **Kostentragung**. Eine Verpflichtung zum BYOD ohne finanzielle Entschädigung wäre AGB-rechtlich unzulässig und damit unwirksam. Etwa Telefoniekosten für betrieblich veranlasste Gespräche sind zwingend vom Arbeitgeber zu tragen.

Zu klären sind auch **Haftungsfragen**. Bei **Schäden des Arbeitgebers**, die durch Fehler des Arbeitnehmers entstehen, greifen die Grundsätze zur beschränkten Arbeitnehmerhaftung. Das heißt im Wesentlichen, dass ein Arbeitnehmer nur beschränkt entsprechend dem Grad seines Verschuldens haftet.[2] Denkbar sind etwa Fälle, in denen dem Arbeitgeber durch Virenbefall ein Schaden entsteht, weil der Arbeitnehmer sein System nicht angemessen vor Viren schützt. Bei **Schäden des Arbeitnehmers** (Beschädigung oder Abhandenkommen) kommt in Betracht, dass der Arbeitgeber diese nach § 670 BGB erstatten muss. Entscheidend ist insoweit, ob der Schaden bei der privaten oder bei der betrieblichen Nutzung eingetreten ist. Diese Abgrenzung ist oft schwierig. In bestimmten Grenzen ist es möglich, Haftungsgrenzen vertraglich zu pauschalieren. Sinnvoller kann der Abschluss einer Geräteversicherung sein.

Ferner zu bedenken ist auch die **Art** und **Weise** und **Umfang** der Nutzungspflicht und Möglichkeiten der **Beendigung** der Nutzungspflicht.

Zu regeln sind auch **Zugriffsmöglichkeiten** des Arbeitgebers auf das Equipment des Arbeitnehmers. Entsprechendes gilt für Einschränkungen der **Verfügungsbefugnis** des Arbeitnehmers. Grundsätzlich

[1] *Franck* RDV 2013, 185, 188
[2] BAG 22.06.2011 – 8 AZR 102/10

darf er mit seinem Eigentum tun und lassen, was er will. Dieses Recht bedarf ggf. einer Einschränkung, etwa in Bezug auf das Herunterladen unsicherer Software.

Weiter sollten **Verhaltenspflichten** zur Einhaltung der nötigen Sicherheitsstandards geregelt werden (Passwortschutz, regelmäßige Updates, Virenschutz, Verbot von Cloud-Diensten und Jailbreaks).

Auch ein **Herausgabeanspruch** sollte geregelt werden. Dieser muss jedoch in Bezug auf seine Voraussetzungen (interne Untersuchungen o.ä.) klar geregelt werden. Auch die Pflicht zur Herausgabe aller Arbeitgeberdaten, die bei der Beendigung des Arbeitsverhältnisses auf dem privaten Device gespeichert sind, sollte geregelt werden.

Ein Regelungsbedürfnis besteht auch in Bezug auf die **Arbeitszeit**. So folgt etwa aus der betrieblichen Nutzung des Privathandys praktisch die ständige Erreichbarkeit des Arbeitnehmers. Das kann problematisch sein im Hinblick auf die Einhaltung der Ruhezeit gemäß § 5 Arbeitszeitgesetz (ArbZG), Pausenzeiten (§ 4 ArbZG) oder Höchstarbeitszeiten (§ 2 ArbZG). Außerdem ist zu klären, ob mit der betrieblichen Nutzung des Handys ein Rufbereitschaftsdienst verbunden werden soll. Auch im Urlaub des Arbeitnehmers ist problematisch, dass das Verlangen einer (auch nur kurzfristigen) Arbeit den Urlaubstag zu einem Arbeitstag macht und damit der Urlaubstag nicht verbraucht wird.

Merke: „*BYOD*“ muss mit Arbeitnehmern vereinbart werden. Bei der Vereinbarung sind zahlreiche Aspekte zu beachten.

3. Datenschutzrecht

Problematisch sind häufig datenschutzrechtliche Fragen. Das hängt davon ab, welche Daten der Arbeitnehmer auf seinem privaten Device nutzt. Neben dem Bundesdatenschutzgesetz und der DS-GVO kommt in Betracht, dass der Arbeitgeber als „*Diensteanbieter*“ im Sinne des § 3 Nr. 10 Telekommunikationsgesetz (TKG) zu betrachten ist. Das ist etwa der Fall, wenn er die SIM-Karte für ein Handy stellt. Dann richten sich Zugriffsrechte nach dem TKG und es drohen nicht unerhebliche Strafbarkeitsrisiken, wenn man gegen die entsprechenden Pflichten verstößt (§ 206 StGB). Das TKG verlangt insbesondere separate Einwilligungserklärungen des betroffenen Arbeitnehmers.

4. Mitbestimmungsrechte des Betriebsrats

In aller Regel sind bei der Einführung von BYOD Mitbestimmungsrechte des Betriebsrats zu beachten. Stellt das BYOD-Modell Verhaltensregeln auf, etwa die Nutzung eines Viren- oder Passwortschutzes, ist das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG (Ordnungsverhalten) einschlägig.

Wird BYOD zu einer ständigen Erreichbarkeit bzw. Rufbereitschaft eingesetzt, sind die Mitbestimmungsrechte des § 87 Abs. 1 Nr. 2 (Beginn und Ende der Arbeitszeit) und § 87 Abs. 1 Nr. 3 BetrVG (Änderung der betrieblichen Arbeitszeit) einschlägig.

Wird dem Arbeitgeber die Möglichkeit eingeräumt, das Verhalten der Mitarbeiter zu überwachen, greift das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Das kommt etwa in Betracht, wenn Zugriffsrechte geregelt werden oder die Festplatte des Mitarbeiters mittels Backup gesichert werden soll. Auch bei der Möglichkeit einer Fernwartung ist das Mitbestimmungsrecht des Betriebsrats zu beachten.

Merke: „*BYOD*“-Modelle lösen mehrere Mitbestimmungsrechte des Betriebsrats aus.

5. Aufbewahrung

Es ist ferner sicherzustellen, dass die gesetzlichen Aufbewahrungspflichten von Unterlagen (etwa § 257 Abs. 1 HGB, § 147 Abs. 1 AO) eingehalten werden können, auch wenn sich die Unterlagen auf den Devices des Arbeitnehmers befinden.

6. Lizenzrecht

Um urheberrechtliche Probleme zu vermeiden (§ 99 UrhG) sollte geprüft werden, welche Lizenzen der Arbeitnehmer auf seinem System nutzt. Privatlizenzen von Software erlauben in der Regel nicht auch die berufliche Nutzung, insofern müssen unter Umständen zusätzliche Lizenzen erworben werden.

Wenn Sie bei der Einführung von BYOD oder der Gestaltung von BYOD-Vereinbarungen oder der Verhandlung von BYOD-Betriebsvereinbarungen Hilfe benötigen, wenden Sie sich jederzeit gern an mich.

Dr. DANIEL WEIGERT, LL.M. (Lund)
Rechtsanwalt · Fachanwalt für Arbeitsrecht
Data Protection Risk Manager

Ballindamm 6 · 20095 Hamburg
t +49 40 668 916 32 · f +49 40 668 916 33
dw@danielweigert.de · www.danielweigert.de