BETRIEBSRÄTE-INFO 10/2018

GEWERKSCHAFT
DER JOURNALISTINNEN
UND JOURNALISTEN
DEUTSCHER
JOURNALISTEN-
VERBAND
BENNAUERSTRASSE 60
53115 BONN
TEL. 02 28 - 2 01 72 11
TELEFAX 02 28 - 2 01 72 32
E-MAIL: DJV@DJV.DE
INTERNET: WWW.DJV.DE

25. Oktober 2018

BYOD = Bring Your Own Device

Einige Betriebsräte müssen sich mit dem Ansinnen des Arbeitgebers befassen, dass Endgeräte nicht vom Arbeitgeber angeschafft werden, sondern Mitarbeiter sollen verpflichtet werden, ihre eigenen Smartphones oder Tablets zu nutzen (BYOD).

Es kann niemand verpflichtet werden, diese privaten Endgeräte für dienstliche Zwecke einzusetzen; denn gemäß § 618 Bürgerliches Gesetzbuch (BGB) hat der Arbeitgeber die Gerätschaften anzuschaffen und so zu unterhalten, dass der Arbeitnehmer gegen Gefahr für Leib, Leben und Gesundheit geschützt ist. Diese dem Arbeitgeber obliegenden Verpflichtungen können auch nicht im Voraus durch Vertrag aufgehoben oder beschränkt werden (619 BGB).

Datenschutz

Aber auch Datenschützer sind über BYOD nicht erfreut. Der Arbeitgeber bleibt für die Umsetzung des Datenschutzes verantwortlich, auch dann, wenn die Mitarbeiter für die Arbeit eigene Geräte benutzen. Das galt schon immer, aber die Datenschutz-Grundverordnung (DSGVO) hat das Bußgeld seit Mai 2018 deutlich erhöht. Es beträgt bis zu 20 Mio. Euro oder bis zu vier Prozent des Jahresumsatzes. Eine weitere Neuerung ist, dass man nicht warten muss, bis eine Datenpanne vorliegt, sondern die Strafen schon dann verhängt werden können, wenn ein Unternehmen keine Maßnahmen zum Datenschutz oder zur Datensicherheit nachweisen kann. Die Firmen tun eher gut daran sicherzustellen, dass die Daten immer auf dem Firmenserver bleiben und z. B. einen so genannten Virtual Private Network-Zugang (VPN) anzubieten. Dies hat zur Folge, dass der Mitarbeiter zwar Daten einsehen und bearbeiten, aber nicht auf dem eigenen Gerät speichern kann.

WhatsApp-Firmengruppen sollten tabu sein, denn WhatsApp ist nicht DSGVO-konform zu gestalten. Selbst wenn die Mitarbeiter diese App ausschließlich privat nutzen, dürfen sie keine Kundendaten auf dem Handy speichern, denn der Messengerdienst von WhatsApp greift automatisch auf alle Kontakte zu, die im Adressbuch gespeichert sind. Das ist ein Verstoß gegen den Datenschutz. Lösen lässt sich das Problem nur, wenn eine so genannte Containerlösung gewählt wird. Dies sorgt dafür, dass WhatsApp nicht mehr auf Daten außerhalb dieses Bereiches zugreifen kann. Datenschützer empfehlen daher die Nutzung von zwei Handys, ein privates und ein Dienstsmartphone. Um den Datenschutz bei der Nutzung privater Endgeräte zu sichern, müssen folgende Punkte geregelt werden:

- Der Mitarbeiter muss einen Passwortschutz und einen Virenscanner auf dem Privatgerät installieren.
- Es muss mit Verschlüsselung gearbeitet werden.

- Mitarbeiter dürfen berufliche E-Mails nicht an ihren Privataccount weiterleiten.
- Mitarbeiter dürfen keine Daten aus dem Firmennetzwerk herunterladen und speichern.
- Mitarbeiter dürfen ihre Endgeräte nur nutzen, wenn sichergestellt ist, dass niemand mitliest. Wer im Biergarten oder im Flugzeug arbeitet, muss sicherstellen, dass niemand über die Schulter mitlesen kann. Man braucht also einen Blickschutzfilter, sobald man in der Öffentlichkeit an derartigen Geräten arbeitet. Letzteres gilt auch für Firmenlaptops.

Kommen personenbezogene Daten abhanden, weil das Endgerät verloren geht oder gestohlen wird, so haftet gemäß § 82 DSGVO das Unternehmen gegenüber dem Geschädigten. Unter Umständen kann der Arbeitgeber beim Arbeitnehmer nach den Regeln der Arbeitnehmerhaftung Regress nehmen, z. B. wenn Kundendaten an Dritte verkauft wurden oder der Arbeitnehmer grob fahrlässig gehandelt hat, indem z. B. eine vorgeschriebene Sicherheitssoftware nicht installiert wurde, ohne Virenschutz gearbeitet wurde oder Daten unverschlüsselt und ohne Passwortschutz auf mobile Datenträger kopiert wurden.

Mögliche Inhalte einer Betriebsvereinbarung

1. Die IT der Firma bestimmt die zulässigen Geräte für den Zugriff auf die Unternehmensdaten und Anwendungen für die dienstliche Nutzung privater mobiler Endgeräte (Smartphones, Tablets). Die Sicherheitsvorkehrungen, die von der IT festgelegt wurden, sind einzuhalten.

2. Die Nutzung von privaten mobilen Geräten erfolgt freiwillig und auf Wunsch des Mitarbeiters. Die Nutzung von BYOD kann daher nur vom Mitarbeiter initiiert werden. Zur Freiwilligkeit gehört auch, dass der Mitarbeiter ohne jede Begründung jederzeit aus der Nutzung von BYOD aussteigen kann.

3. Es besteht keine Verpflichtung, auf Mails oder Telefonate, Facebook- oder Twittermeldungen o. ä. außerhalb der Arbeitszeit zu antworten.

4. Die Zustimmung des Vorgesetzten muss eingeholt werden. Die Zustimmung ist von Vorgesetzten zu erteilen, wenn für den betreffenden Redakteur/die Redakteurin ein mobiler Zugang zu Unternehmensdaten sinnvoll ist. Dabei sind die betrieblichen Belange zu berücksichtigen.

5. Für die Nutzung privater mobiler Geräte werden dem Redakteur/der Redakteurin monatlich XXX Euro erstattet.

6. Bei Streitigkeiten über Auslegung oder Anwendung der Betriebsvereinbarung können Redakteur/Redakteurin oder eine der Betriebsparteien eine innerbetriebliche Clearingstelle einberufen. Diese Clearingstelle besteht aus je zwei Vertretern des Betriebsrats und der Geschäftsleitung.

7. Eine Überwachung der Redakteurin/des Redakteurs findet nicht statt. Die Firma verpflichtet sich, mögliche Erkenntnisse aus einer Verhaltens- und Leistungsüberwachung nicht für arbeitsrechtliche Maßnahmen zu nutzen.

Redaktion: Gerda Theile
☏ 0228/2 01 72 11; E-Mail: the@djv.de