Perpetuum Mobility

MOBILE DEVICES *Aufgabe von Betriebs- und Personalräten ist es, die Gefahren beim beruflichen Einsatz von Smartphones und deren Verwaltungssoftware zu erkennen. Mindestregelungsinhalte in Vereinbarungen ziehen Grenzen und sensibilisieren die Belegschaft.*

VON **ACHIM THANNHEISER**

Ein Perpetuum Mobile ist etwas »sich ständig Bewegendes«. Die Sehnsucht nach dem Gerät, das – einmal in Gang gesetzt – ohne weitere Energiezufuhr ewig in Bewegung bleibt, erfüllen auch mobile Geräte nicht. Aber sie vermitteln den Eindruck, dass die User ständig in »Bewegung« bleiben. Dies werden die Betriebs- und Personalräte im Rahmen der Mitbestimmung nicht verhindern können, aber krankheitsfördernder Nutzung und ständiger Kontrolle können sie Grenzen setzen.

Entscheidende Fragen

Was wird mit mobilen Geräten gearbeitet? Fast gilt ja schon, dass es kaum noch etwas gibt, was zumindest im Dienstleistungsbereich nicht mit mobilen Geräten bearbeitbar ist. Dagegen ankämpfen zu wollen, erscheint sinnlos. Nicht nur weil das der Unternehmensrealität widerspricht, sondern auch, weil es die Kolleginnen und Kollegen wollen. Denn besonders junge Beschäftigte, die mit der Nutzung von Smartphones aufgewachsen sind, werden nicht davor zurückscheuen, Unternehmensdaten auf Privatgeräten zu speichern, wenn diese sich hierdurch einen Produktivitätsgewinn oder mehr Komfort bei der Arbeit versprechen.[1]

Was können die mobilen Geräte? Weit mehr als PCs noch vor zehn Jahren konnten, was die Leistung der Chips betrifft. Sie sind beispielsweise Kamera, GPS- und Videogerät, Arbeitsbildschirm, Chatgerät und schließlich auch Telefon. Damit wird deutlich, nur im Rahmen von Leistungs- und Verhaltenskontrolle zu denken, greift zu kurz. Gesundheitsschutz in Bezug auf ständige Erreichbarkeit[2] und vor allem Ergonomie[3] ist ein zentrales Thema. Dessen Lösung ist sicher nicht mit Verboten erreichbar, sondern vor allem mit Qualifizierung der Anwender.

Was kann die Geräte- und insbesondere die Verwaltungssoftware der Geräte? Es gibt die verschiedensten Systeme. Unter Enterprise Mobility Management (EMM) werden die drei Teilaspekte Mobile Device Management (MDM), Mobile Application Management (MAM) und Mobile Information Management (MIM) zusammengefasst.[4] Ortung, Beobachtung und umfassende Auswertungsmöglichkeiten aller Aktivitäten der Nutzer sind die Stichworte dazu.

Wer kontrolliert den Einsatz und die Auswertung der Arbeit mit mobilen Geräten? Es werden inzwischen standardmäßig Möglichkeiten für die Geräte angeboten, um die Erreichbarkeit und Ortung eines Mobilgeräts einzuschränken.[5] Diese müssen aber auch umgesetzt und beispielsweise über Betriebs- oder Dienstvereinbarungen kontrolliert werden. Eine zentrale Aufgabe der Belegschaftsvertretung.

Aufgaben der Mitbestimmung

Aufgabe von Betriebs- und Personalräten ist es, die Risiken zu bestimmen und zu begrenzen. Es geht heute auf einfache Weise schon sehr viel, was vor wenigen Jahren noch wegen eines zu hohen technischen Aufwands abgelehnt wurde. So beschreiben Christian Neßlinger und Heinz-Peter Höller, dass bei mobilen Geräten mit Arbeitsprofil, dieses durch den User deaktiviert werden kann. Ist das Profil deaktiviert, werden keine Anwendungen, die im Arbeitsprofil hinterlegt sind, ausgeführt.[6] Damit würden Beschäftigte in ihrer dienst-

DARUM GEHT ES

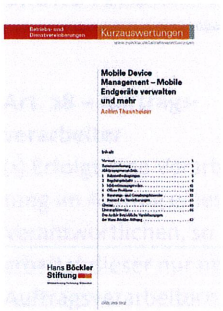
1. Der Einsatz von mobilen Endgeräten bei der Arbeit braucht Regeln.

2. Ein besonderes Augenmerk ist auf Kontrolle, Ergonomie und Datenschutz zu richten.

3. Die Belegschaft ist im Umgang mit den Mobile Devices zu schulen.

1 Vgl. Neßlinger / Höller, Mobilgeräte im betrieblichen Einsatz, in: CuA 3/2018, 8 ff. in diesem Heft
2 Vgl. Wedde, Den Arbeitsplatz immer dabei, in: CuA 11/2016, 8 ff. und ders., »Mobile Work« – immer und überall arbeiten können, in: CuA 9/2015, 4 ff.
3 Vgl . Wallbruch / Hess / Weddige, Mobile Arbeit, computing anywhere, Heft 84, www.tbs-nrw.de/fileadmin/Shop/Broschuren_PDF/Mobile_Arbeit.pdf
4 Dazu ausführlich Neßlinger / Höller, aaO., 8 ff. (9)
5 Vgl. Neßlinger / Höller, aaO., 8 ff. (11)
6 Vgl. Neßlinger / Höller, aaO., 8 ff. (11)

LESETIPP



Mobile Endgeräte verwalten
Die Hans-Böckler-Stiftung hat 21 betriebliche Vereinbarungen zum Mobile Device Management durch den CuA-Autor Achim Thannheiser auswerten lassen und die Ergebnisse für Regelungen in der Praxis zusammengestellt.
www.boeckler.de

freien Zeit nicht durch Benachrichtigungen von geschäftlichen Anwendungen gestört und ebenso könnten GPS-Dienste privat genutzt werden, ohne dass diese der Arbeitgeber auslesen kann.[7]

Als Durchsetzungsinstrumente stehen den Mitbestimmungsgremien die verschiedenen Beteiligungsrechte zur Seite.[8] An erster Stelle ist die Mitbestimmung bei der Leistungs- und Verhaltenskontrolle mit technischen Einrichtungen (§ 75 Abs. 3 Nr. 17 BPersVG und § 87 Abs. 1 Nr. 6 BetrVG) zu nennen. Dafür reicht es aus, dass die Beschäftigten befürchten müssen, während der Arbeit mit Hilfe technischer oder elektronischer Kontrolleinrichtung jederzeit beobachtet oder in anderer Weise fortlaufend kontrolliert zu werden. Dieser entstehende Überwachungsdruck behindert die Beschäftigten in der freien Entfaltung ihrer Persönlichkeit.[9] Damit ist dies auch der Ansatz für datenschutzrechtliche Fragen, soweit in den Ländern nicht spezielle Regelungen bestehen – zum Beispiel § 75 Abs. 4 Nr. 16 des baden-württembergischen Landespersonalvertretungsgesetzes (BaWüPersVG).

Eine mitbestimmungspflichtige technische Überwachungseinrichtung liegt schon vor, wenn die Einrichtung es ermöglicht, das Verhalten oder die Leistung von Beschäftigten zu überwachen, ohne dass dies konkret gewollt oder eine App installiert sein muss.[10] Damit ist also nicht danach zu fragen, was hat der Arbeitgeber vor, sondern was könnten Geräte und EMM.

Die Mitbestimmung beim Arbeits- und Gesundheitsschutz ist als ausfüllungsbedürftige Rahmenvorschrift in § 3 Arbeitsschutzgesetz (ArbSchG) konzipiert, § 75 Abs. 3 Nr. 11 BPersVG und § 87 Abs. 1 Nr. 7 BetrVG. Dabei ist es die Aufgabe entsprechender Regelungen nicht nur physische, sondern auch psychische Beanspruchungen zu vermeiden, in jedem Fall aber zu minimieren.[11]

Ein weiteres zentrales Mitbestimmungsinstrument ist die Beteiligung bei Regelungen zur Arbeitszeit, § 75 Abs. 3 Nr. 1 und Abs. 4 BPersVG und § 87 Abs. 1 Nr. 2 und 3 BetrVG. Dazu gehören Fragen zur Verteilung (täglich, wöchentlich), zu Pausen, Rufbereitschaft, Mehrarbeit / Überstunden, Dienstreisen und -plänen.

Schließlich wird über die Beteiligungsrechte zu Qualifizierungsmaßnahmen die Fähigkeit der Beschäftigten zur angemessenen und richtigen Nutzung mobiler Geräte erreichbar, § 75 Abs. 3 Nr. 6 und 7 BPersVG und §§ 96 ff. BetrVG.

Regelungsmöglichkeiten in einer Vereinbarung

Die Beteiligungsrechte werden in Betriebs- oder Dienstvereinbarungen umgesetzt. Dabei ist auf die eingesetzten mobilen Geräte und die jeweilige Verwaltungssoftware abzustellen. Daher gibt es »die eine« Vereinbarung nicht. Mindestregelungsinhalte sollen jedoch nachfolgende Beispiele aufzeigen.

▸ Mobile Geräte

Gegenstand: Diese Vereinbarung hat den Einsatz, die Nutzung und die ortsunabhängige Arbeit mit mobilen Endgeräten zum Gegenstand. Mobile Endgeräte in diesem Sinne sind Handy, Smartphone, Tablet-PC und Laptop.

Zielsetzung: Ziele dieser Vereinbarung sind Regelungen zur Nutzung, Sicherheit, Ergonomie, Freiwilligkeit und Qualifizierung für mobiles Arbeiten und die Arbeit mit mobilen Endgeräten. Ziele sind weiter der Schutz der Firmendaten, der privaten Daten und personenbezogenen Daten. Auf die Belange schwerbehinderter und gleichgestellter Menschen wird besonders Rücksicht genommen.

Datenschutz: Für das Erheben, Verarbeiten und Nutzen personenbezogener oder personenbeziehbarer Daten gelten die Grundsätze der Verhältnismäßigkeit und Zweckbindung. Ersterer bedeutet, so wenig Daten wie möglich im Hinblick auf die Zwecksetzung dieser Vereinbarung zu erfassen und zu verarbeiten und Letzterer das Verbot der Datenverarbeitung und -nutzung zu nicht in dieser Vereinbarung festgelegten Verwendungszwecken.

Schutz der Gerätedaten: Das mobile Endgerät ist zwingend mit einem Passwort oder einer vergleichbaren Zugangssperre zu sichern. Das Passwort ist geheim zu halten und die Weitergabe des Passwortes ist untersagt.

Persönliche Daten: Soweit Beschäftigte private Daten in von der Firma zur Verfügung gestellte Apps, dienstlichen Mail-Accounts oder den dienstlichen Kalender der Firma übernehmen, werden diese auch dienstlich gespeichert. Die Beschäftigten werden informiert, dass ihre persönlichen Daten im Übrigen nicht gesichert werden und bei einem Geräteverlust oder ei-

7 So berichten Neßlinger / Höller, aaO., 8 ff. (12)
8 Dazu Thannheiser, Mobile Kommunikation, in: CuA 2/2014, 4 ff.; Höller/Thannheiser, Mobile Device Management, in: CuA 11/2015, 4 ff.
9 BAG 7.10.1987 – 5 AZR 116/86; BAG 29.6.2004 – 1 ABR 21/03; BVerwG 31.8.1988 – 6 P 35/85
10 BVerwG 24.9.1991 – 6 P 6/90
11 LAG Hamm 9.3.2012 – 13 TaBV 100/10

nem notwendigen Löschen der Daten auf den mobilen Geräten verloren gehen.

Durchführungs- und Verwertungsverbot: Eine Leistungs- und Verhaltenskontrolle findet nicht statt. Werden personenbezogene Daten unzulässig verarbeitet oder genutzt, besteht diesbezüglich ein vollständiges Verwertungsverbot. Eine Ortung des mobilen Endgeräts durch die Firma wird nicht durchgeführt. Ausnahmen hiervon sind die Ortung nach Verlust oder Diebstahl oder staatliche Anordnung. Der Firma ist ein Zugriff auf private Daten nicht gestattet, soweit nicht gesetzliche Erlaubnistatbestände dies gestatten oder der Beschäftigte vorher eine Einverständniserklärung abgegeben hat.

Arbeitszeitgrenzen: Die Nutzung der mobilen Endgeräte ist zu dienstlichen Zwecken außerhalb der individuellen Arbeitszeit im Rahmen der betrieblichen Arbeitszeitvereinbarungen freiwillig. Außerhalb ihrer individuellen Arbeitszeit sind die Beschäftigten berechtigt, das Gerät auszuschalten. Die Beschäftigten haben bei der Nutzung der mobilen Endgeräten darauf zu achten, dass sie die gesetzlichen – insbesondere das Arbeitszeitgesetz – und die durch betriebliche Vereinbarungen bestimmten Arbeitszeitregelungen einhalten. Die Nutzung mobiler Geräte ersetzt keine Rufbereitschaft und führt zu keiner Erreichbarkeit der Beschäftigten außerhalb ihrer persönlichen Arbeitszeit. Es gelten unverändert die betrieblichen Regelungen zur Arbeitszeit, Mehrarbeit, Rufbereitschaft und Überstunden. Die Arbeit mit mobilen Geräten ist Arbeitszeit. Der Arbeitgeber stellt eine einfache technische Lösung zum Erfassen der Arbeitszeit für die Arbeit mit mobilen Geräten zur Verfügung. Der Betriebsrat erhält monatlich eine Übersicht über die Arbeitszeiten mit mobilen Geräten der Arbeitnehmer.

Blacklist: Eine Liste von (aktuell) nicht zugelassenen Apps wird jeweils aktuell im IT-Nutzerhandbuch bereitgestellt. Diese Apps werden systembedingt nicht zugelassen. Das Herunterladen von Spielen und Apps mit pornographischen, menschenverachtenden oder extremistischen Inhalten ist verboten.

Qualifikation: Die Beschäftigten erhalten verpflichtend die für den Einsatz und die Anwendung der mobilen Endgeräte sowie der Apps notwendigen und geeigneten Qualifizierungsmaßnahmen. Diese umfassen insbesondere die folgenden Aspekte:

- Anforderungen an einen möglichst gesundheitsverträglichen Umgang mit mobilen Geräten.
- Schulung zu den physischen und psychischen Gefahren bei der Arbeit mit mobilen Geräten.
- Beachtung, Einhaltung und Umgang mit den Sicherheitsanforderungen.
- Einbindung der mobilen Endgeräte als Arbeitsgerät in die bestehenden Arbeitsabläufe.

Haftungsbegrenzung: Die Mitarbeiter haften für Schäden an den mobilen Endgeräten und für den Verlust der mobilen Endgeräte nur bei grober Fahrlässigkeit bis maximal 100 Euro (Versicherungslösung) und bei Vorsatz.

▸ Verwaltungssoftware

EMM-System: Die Funktions- und Systembeschreibung des Enterprise Mobility Management (EMM) inklusive Server und alle jeweils genutzten Teilkomponenten und technischen Prozessabläufe sind in der Anlage geregelt.

Administration: Die Administratoren haben Zugriff auf die Konfigurationsdaten, Sicherheitsrichtlinien und Log-Daten, die in der SQL-Datenbank des Systems gespeichert werden. Das Rollen- und Berechtigungskonzept ist in der Anlage abschließend beschrieben.

Datenverlust: Die Beschäftigten sind ausdrücklich darauf hinzuweisen, dass durch den Arbeitgeber die technische Möglichkeit besteht, sämtliche auf dem Gerät vorhandenen Daten und Anwendungen aus berechtigten betrieblichen Gründen (Geräteverlust, falsche Code-/Passworteingabe, Sicherheitsvorfälle) zu löschen. Die Beschäftigten haben daher selbst für eine ausreichende Sicherung (Backup) der privaten Daten und Anwendungen Sorge zu tragen.

Personenbezogene Daten: Durch das EMM-System werden folgende Log-Daten pro Mobile Device erfasst und gespeichert:

- Rufnummer
- IMEI und/oder Seriennummer des Geräts
- Zeitpunkt der letzten Synchronisierung des Geräts
- Zeitpunkt der letzten App-Synchronisierung des EMM-Systems
- E-Mail-Adresse des Benutzers (mit Vor- und Nachname)

IMEI

Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert werden kann. Dual-SIM-Handys besitzen zwei IMEI-Nummern. Die IMEI eines Mobiltelefons kann durch die Eingabe *#06# im Eingabefeld der Telefonnummer abgefragt werden.
[Quelle: Wikipedia]

LESETIPP

Mobile Arbeit gestalten
Viele Beschäftigte arbeiten zunehmend dort, wo es der Netzempfang gerade zulässt: orts- und zeitunabhängig mit Hilfe mobiler Endgeräte. Dieses Arbeiten kommt Arbeitgebern entgegen, aber auch Arbeitnehmer schätzen die Vorteile, weil sie so die Arbeit flexibel an ihre Lebenssituation anpassen können. Diese mobile Arbeit zu regeln, stellt die Interessenvertretung vor große Herausforderungen. Die neue Handlungshilfe der TBS Nordrhein-Westfalen »Mobile Arbeit, computing anywhere« hilft dabei. Sie stellt zwei Aspekte in den Mittelpunkt: die Organisation der Arbeit, damit die gesetzlichen Regelungen etwa zur Höchstarbeitszeit, zur Samstagsarbeit oder zu Pausen eingehalten werden können und die technischen Gegebenheiten mobiler Arbeit im Hinblick auf Leistungs- und Verhaltenskontrollen und den Datenschutz. Kostenloser Download: **www.tbs-nrw.de**

Speicherungsdauer: Das Speichern der Log-Daten unterliegt der betrieblichen Aufbewahrungsfrist von maximal 180 Tagen. Die Daten werden anschließend automatisch gelöscht. Die Log-Daten sind ausschließlich von den Administratoren zu Support- und Serviceanfragen einsehbar. Die gespeicherten Log-Daten dürfen nach Ablauf von zwei Monaten nach der Erhebung bezogen auf einzelne Beschäftigte nicht mehr ausgewertet werden. Ausgenommen hiervon sind IMEI- und Seriennummern bei konkreten technischen Problemen an den Systemen, soweit der Vorgang in einem Ticket dokumentiert ist.

Durchführungs- und Verwertungsverbot: Es finden keine personenbezogenen oder personenbeziehbaren Auswertungen statt. Eine Ortung der Endgeräte findet durch die Firma nicht statt.

Remote Control: Eine Fernwartung wird nur im Fehler- und Supportfall eingesetzt, wenn der Anwender dies wünscht und auslöst. Sonst erfolgt in keinem Fall ein Remote-Zugriff auf die Geräte oder Apps.

Aufschaltung: Ein Mithören ohne Zustimmung des Mitarbeiters ist unzulässig. Ebenso ist ein Zugriff auf Kamera oder Mikro und Bildschirmfotos der mobilen Geräte durch die Firma oder Dritte ohne Zustimmung der Beschäftigten unzulässig. Werden personenbezogene Daten unzulässig verarbeitet oder genutzt, besteht diesbezüglich ein vollständiges Verwertungsverbot.

Rufumleitung: Nur die oder der Beschäftigte darf eine Rufumleitung einrichten. Im Krankheitsfall oder anderen längeren Abwesenheitszeiten ist dies durch den Admin zulässig, wenn die betriebliche Interessenvertretung vorab zugestimmt hat und die oder der Betroffene darüber informiert wird. Wenn diese oder dieser einen Missbrauch moniert, ist die Möglichkeit der Rufumleitungsschaltung durch den Admin in diesem Fall zu stoppen.

IT-Rechte: Die installierten Apps sind ausschließlich vom Administrator einzusehen. Dabei wird nur die App selbst gesehen und nicht die Daten, die diese App nutzt. Die Nutzung dieser Sicht ist nur im Service- und Supportfall zulässig und ist in einem Ticket zu dokumentieren.

Datenweitergabe: Technische Schnittstellen ergeben sich beim EMM zu den Firewall-Systemen, Switches und Routern. Die genutzten Schnittstellen sind in der Anlage abschließend aufgeführt. Sämtliche Regelungen dieser Vereinbarung, insbesondere zur Verhältnismäßigkeit und Zweckbindung gelten fort, soweit die Daten über die in der Anlage aufgelistete Schnittstelle in andere Systeme überführt werden.

Kontrolle: Zum Überprüfen der Einhaltung vorgenannter Bestimmungen ist die betriebliche Interessenvertretung jederzeit berechtigt in alle Systeme und Speichermedien Einsicht zu nehmen, Protokolle einzufordern und sachverständige Unterstützung – nach Zustimmung der Firma auch externe Unterstützung – hinzuziehen.

Streitlösung: Bei Uneinigkeit zwischen Arbeitgeber und Arbeitnehmer oder deren Vertretung wird mit dieser über eine einvernehmliche Lösung verhandelt. Dies gilt auch für Sonderregelungen (Untersagung, Einschränkung oder Ausweitung mobiler Arbeit) für einzelne Beschäftigte. Einigen diese sich nicht und bei Beschwerden der Beschäftigten, findet das in § 85 Abs. 2 BetrVG vorgesehene Einigungsstellenverfahren Anwendung.

Fazit

Die dienstliche Nutzung mobiler Geräte gehört heute in breitem Umfang zum Berufsalltag. Die Betriebs- und Personalräte haben dabei die Aufgabe, die mit der Nutzung einhergehenden Gefahren und Risiken für die Beschäftigten soweit wie irgend möglich zu minimieren.

Daher sind Regelungen für den Einsatz der Geräte einerseits und der verwaltenden Software andererseits unumgänglich. Neben dem Verbot von Leistungs- und Verhaltenskontrollen, von Remote-Zugriffen, dem Mithören von Gesprächen oder dem Aufschalten auf das mobile Gerät, gehört auch die »Befähigung« der Beschäftigten zum wichtigsten Regelungsinhalt.

Befähigung meint dabei, dass der Belegschaft die gesundheitlichen Gefahren der falschen Nutzung bewusst wird. Dies soll die Pflicht der Unternehmen, den Gesundheitsschutz für die Beschäftigten umzusetzen, nicht minimieren. ◁

Achim Thannheiser, Rechtsanwalt und Betriebswirt bei Rechtsanwälte Thannheiser & Koll., Hannover
thannheiser@thannheiser.de