Betriebs- und Dienstvereinbarungen

Kurzauswertungen

www.boeckler.de/betriebsvereinbarungen

Mobile Device Management – Mobile Endgeräte verwalten und mehr

Achim Thannheiser

Inhalt

Hans Böckler Stiftung

Mitbestimmung · Forschung · Stipendien

ISSN 1869-3032

Archiv Betriebliche Vereinbarungen

↘ www.boeckler.de/betriebsvereinbarungen

Mobile Device Management – Mobile Endgeräte verwalten und mehr

Achim Thannheiser
Selbständiger Rechtsanwalt und Betriebswirt in Hannover, Schwerpunkt Arbeitsrecht und Beratung von Betriebs- und Personalräten, Fachbuchautor.

Redaktion: Dr. Manuela Maschke, Hans-Böckler-Stiftung
Hans-Böckler-Str. 39, 40476 Düsseldorf
Kontakt: 0211/7778-167, betriebsvereinbarung@boeckler.de
Produktion: Setzkasten GmbH, Düsseldorf
Stand: Juni 2015

Online-Publikation, download unter:
www.boeckler.de/betriebsvereinbarungen

ISSN: 1869-3032

Vorwort

Smartphone und Tablet haben das berufliche und private Leben verändert. Unternehmen fördern die Nutzung. Um mobile Geräte zu verwalten wird inzwischen häufig ein Mobile Device Managements (MDM) eingeführt. Alle mobilen Geräte (Devices) können auf diese Weise mit Softwaresteuerung zentral verwaltet und auch überwacht werden. Durch MDM werden mobile Geräte transparent und auswertbar. Alle mobilen Zugriffe auf Dokumente werden vom MDM-System lückenlos aufgezeichnet. Ob Reihenfolge, Art oder Dauer: Auch die Nutzung von Dokumenten durch Anwender wird erkennbar. Schnittstellen ermöglichen die Weitergabe an beliebige andere Systeme. Die Idee der Verhaltens- und Leistungskontrolle liegt hier nahe.
Die Einführung und Anwendung von MDM-Systemen unterliegt der vollen Mitbestimmung. Sie kann mit einer entsprechenden Betriebs- oder Dienstvereinbarung begleitet werden.
Für die Analyse wurden 21 betriebliche Vereinbarungen ausgewertet. Es wird gezeigt, welche Regelungstrends zur Gestaltung bestehen und wie die betrieblichen Akteure das Thema MDM aufgreifen.
Die Auswertung verfolgt dabei nicht das Ziel, Regelungen zu bewerten, die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen, Hinweise und Anregungen für die Gestaltung eigener Vereinbarungen zu geben.

Weitere Hinweise finden Sie im Internet unter www.boeckler.de/betriebsvereinbarungen.

Wir wünschen eine anregende Lektüre!

Dr. Manuela Maschke

Zusammenfassung

Smartphone und Tablet sind aus unserem Alltag kaum noch wegzudenken. Sie haben das berufliche und private Leben verändert. Die Unternehmen akzeptieren oder fördern die Nutzung dieser mobilen Geräte als Arbeitsplattformen. In den Unternehmen und Verwaltungen wird eine Vielzahl von mobilen Geräten genutzt: unterschiedlichster Hersteller, mit verschiedenen mobilen Endgeräteplattformen (Betriebssystemen) und mit unzähligen Apps. Die dabei üblicherweise eingesetzten Betriebssysteme für mobile Endgeräte umfassen umfangreiche Funktionen a) für die Kommunikation: Telefonie, (Kurz-)Nachrichten und elektronische Post; sowie b) für das persönliche Informationsmanagement: Adressbuch, Kalender und Aufgabenlisten mit umfangreichen Synchronisationsmöglichkeiten. Dazu kommt die unternehmenseigene Infrastruktur mit Firmenkalender, Projektsoftware, firmenweitem Adressbuch, E-Mail und anderen Funktionen.
Um dies alles zu verwalten und die Sicherheitsprobleme in den Griff zu bekommen, bedarf es einer speziellen Software – des Mobile Device Managements (MDM). Es ermöglicht, alle mobilen Geräte (Devices) mit sämtlichen Anwendungen und Konfigurationen zentral zu verwalten und zu überwachen. Durch MDM werden die mobilen Geräte transparent, ortbar und auswertbar – was die Idee der Verhaltens- und Leistungskontrolle nahelegt. Alle mobilen Zugriffe auf Dokumente werden vom MDM-System lückenlos aufgezeichnet. Ob Reihenfolge, Art oder Dauer: Die Nutzung von Dokumenten durch Anwender wird erkennbar. Schnittstellen ermöglichen die Weitergabe an beliebige andere Systeme.
Darüber hinaus ist der sogenannte Echtzeit-Remote-Zugriff möglich – auch Remote-Control genannt: Die Firma, die MDM zur Verfügung stellt oder nutzt, kann sich je nach Freigabe

auf die Mobiltelefone aufschalten und je nach Vereinbarung diese auch fernbedienen. Hierdurch wird sichergestellt, dass Dokumente des Unternehmens bei Verlust oder Diebstahl des mobilen Endgerätes nicht in die Hände Unberechtigter geraten. Ferner wird sichergestellt, dass nicht einmal Spuren von Daten auf dem mobilen Gerät verbleiben. Per Remote-Zugriff können die Daten des mobilen Gerätes bei Verlust oder Diebstahl sofort gelöscht werden. Darüber hinaus sind der Datenschutz sowie die Sicherheit vor Zugriffen Unberechtigter auf interne Informationen gewährleistet. Wurden private Apps nach der Installation von MDM aufgespielt, sind auch sie sowie die dazugehörigen Daten nach einer Fernlöschung nicht mehr vorhanden.
Die Einführung und Anwendung von MDM-Systemen unterliegt der vollen Mitbestimmung. Sie kann mit einer entsprechenden Betriebs- oder Dienstvereinbarung begleitet werden. Die bestehenden Vereinbarungen zu Informationssystemen, Telefonanlagen und zum Arbeiten mit mobilen Geräten genügen nicht für eine umfassende und vollständige Regelung bzw. erfassen nicht die neuen, durch MDM hervorgerufenen Problemstellungen. Die ersten 21 MDM-Vereinbarungen wurden ausgewertet, die Ergebnisse zum vorliegenden Trendbericht für Regelungen in der Praxis zusammengestellt.
Sichtbar wird: Nur wenige Vereinbarungen erfassen das Thema vollständig und decken es gänzlich ab. Unklar bleibt: Woran liegt das? An der permanenten Weiterentwicklung der MDM-Softwareprogramme? An mangelnder Transparenz der MDM-Möglichkeiten für die Betriebs- und Personalräte? Viele Regelungen zeugen von großem Vertrauen in die rechtmäßige Verwendung der MDM-Systeme und/oder fehlendem Problembewusstsein bei den betrieblichen Akteuren. In Kapitel 5.1 werden die Regelungsbreite und die notwendigen Regelungsinhalte aufgezeigt.

Abkürzungsverzeichnis

App	Application
ArbSchG	Arbeitsschutzgesetz
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BPersVG	Bundespersonalvertretungsgesetz
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BYOD	Bring your own device
GG	Grundgesetz
GPS	Global Positioning System
IT	Informationstechnik
IuK	Information und Kommunikation
MDM	Mobile Device Management
SMS	Short Message Service

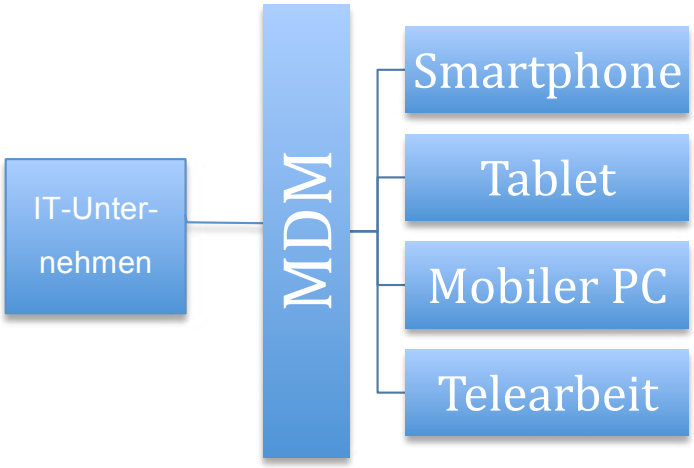
1 Rahmenbedingungen

Das berufliche und private Leben der meisten Menschen ist durchdrungen von der Nutzung des Smartphones und des Tablets (→ Glossar). Die Unternehmen haben die mögliche zusätzliche Leistungsbereitschaft erkannt und akzeptieren oder fördern die Nutzung dieser mobilen Geräte als Arbeitsplattformen. Stellen wir uns ein Versicherungsunternehmen vor: Es stattet alle Innendienstbeschäftigten mit einem Smartphone aus und den Außendienst zudem mit einem Tablet. Nehmen wir weiter an, dass dieses Unternehmen 5.000 Beschäftigte hat und somit mindestens 5.000 mobile Geräte verwalten und administrieren muss. Dafür wurde eine spezielle Verwaltungssoftware entwickelt: das Mobile Device Managementsystem (MDM, → Glossar). Dessen Möglichkeiten werden nachfolgend skizziert und die ersten Reaktionen der Mitbestimmungsgremien in Form von Richtlinien, Betriebs- und Dienstvereinbarungen dazu analysiert.

Bei genauerem Hinsehen, ist zu erkennen: In den Unternehmen und Verwaltungen wird eine Vielzahl von mobilen Geräten unterschiedlicher Hersteller mit verschiedenen mobilen Endgeräteplattformen (Betriebssystemen) eingesetzt: Apple (iPhone und iPad), BlackBerry, Android, Symbian, Windows Phone, Windows Mobile. Schon diese Vielfalt ist für die IT-Administratoren in den Unternehmen schwer zu handhaben. Mobile Geräte werden mittels Mobilfunk oder Internet an das MDM-System angebunden; damit kann der Administrator auf alle Geräte zugreifen, auch wenn diese physisch nicht in erreichbarer Nähe sind (vgl. Steinwender 2013). Die dabei üblicherweise eingesetzten Betriebssysteme für mobile Endgeräte umfassen umfangreiche Funktionen a) für die Kommunikation: Telefonie, (Kurz-)Nachrichten und elektronische Post; sowie b) für das persönliche Informationsmanagement: Adressbuch, Kalender und Aufgabenlisten mit umfangreichen Synchronisationsmöglichkeiten. Dazu kommt die unternehmenseigene Infrastruktur mit Firmenkalender, Projektsoftware, firmenweitem Adressbuch, E-Mail und weiteren Funktionen. Alle aktuellen Betriebssysteme für mobile Endgeräte bieten darüber hinaus Funktionen der Wiedergabe von Audio- und Videodaten. Dies reicht von der Aufzeichnung und Wiedergabe kurzer Diktate bis hin zur hochauflösenden Wiedergabe von Spielfilmen auf dem Bildschirm des mobilen Endgeräts. Dieses ist meist mit einer Kamera ausgestattet und kann in der Regel auch Fotos und Filme aufzeichnen. Darüber hinaus gibt es unzählige Apps (→ Glossar), die auf die mobilen Geräte geladen werden können.

Um dies alles zu verwalten und die Sicherheitsprobleme in den Griff zu bekommen, bedarf es einer speziellen Software – des Mobile Device Managements (MDM). Es ermöglicht, alle mobilen Geräte (Devices) mit sämtlichen Anwendungen und Konfigurationen zentral zu Verwaltung und zu überwachen. Das System kann viele Aufgaben übernehmen:

- Administration von Sicherheitsrichtlinien
- Verteilung von Rollen und Rechten
- Konfigurationen (Apps zulassen, kontrollieren und ggf. löschen)
- Lokalisierung
- Kosten ermitteln und verteilen
- Remote-Control (Fernsteuerung, → Glossar)
- Remote-Support (Fernwartung, → Glossar)
- Inventarisierung der gesamten mobilen Geräte.



Quelle: eigene Darstellung

Bedeutung für die Beschäftigten

Durch MDM werden die mobilen Geräte transparent, ortbar und auswertbar – was die Idee der Verhaltens- und Leistungskontrolle nahelegt. Alle mobilen Zugriffe auf Dokumente werden vom MDM-System lückenlos aufgezeichnet. Ob Reihenfolge, Art oder Dauer: Die Nutzung von Dokumenten durch Anwender wird erkennbar. Schnittstellen ermöglichen die Weitergabe an beliebige andere Systeme. Darüber hinaus ist ein sogenannter Echtzeit-Remote-Zugriff möglich. Die Firma, die MDM zur Verfügung stellt oder nutzt, kann sich je nach Freigabe auf die Mobiltelefone aufschalten und je nach Vereinbarung diese auch fernbedienen. Hierdurch wird sichtbar, was auf dem mobilen Gerät gerade passiert, Verläufe und gespeicherte Daten sind zugänglich. Per Remote-Zugriff lassen sich die Daten des mobilen Gerätes bei Verlust oder Diebstahl sofort löschen; der Datenschutz sowie die Sicherheit vor Zugriffen Unberechtigter auf interne Informationen sind gewährleistet. Wurden private Apps nach der Installation des MDM aufgespielt, sind diese und die dazugehörigen Daten bei einer Fernlöschung (Kill-Befehl) ebenso verloren.
Die MDM-Systeme ermöglichen die Überwachung, Lokalisierung und den Remote-Support des gesamten Geräteparks eines Unternehmens. Für jede Anwendung (App) können dezidierte Berechtigungen vergeben werden: Wer darf welche Netze nutzen? Welche Datensicherungskonzepte gelten? Welche Geräte werden mit welcher Gerätesoftware ausgestattet? Dabei können Geräte zu Gruppen zusammengefasst oder benutzerspezifisch angepasst werden.

Mitbestimmung

Die Einführung und Anwendung von MDM-Systemen unterliegt der vollen Mitbestimmung, da stets Leistungs- und Verhaltenskontrollen möglich sind. Sie kann mit einer entsprechenden Betriebs- oder Dienstvereinbarung begleitet werden. Die bestehenden Vereinbarungen zu Informationssystemen, Telefonanlagen und zum Arbeiten mit mobilen Geräten genügen nicht, da sie meist weder Fernzugriffe noch die durch MDM gegebene Auswertungsvielfalt regeln. Die ersten 21 Vereinbarungen wurden ausgewertet, die Ergebnisse zum vorliegenden Trendbericht für Regelungen in der Praxis zusammengestellt.

2 Regelungsinhalte

Zu Beginn einer Vereinbarung werden meist ihr Grund, ihr Anlass und ihr Umfang beschrieben. Die Inhaltsangabe dient als erste Information für die Beschäftigten, an die sich die Betriebsvereinbarung richtet und deren Schutz ein Hauptzweck ist. Ganz allgemein auf die

Einführung der MDM-Software als Grund für die Vereinbarung abzustellen, führt nur oberflächlich in das Thema ein und setzt voraus, dass der Begriff MDM eingeordnet werden kann.

> „Gegenstand dieser Betriebsvereinbarung ist die Einführung, Nutzung und Weiterentwicklung der Mobile Device Management-Software [Firma], (im folgenden ‚[Firma]' genannt)."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

In einer anderen Vereinbarung wird an dieser Stelle erklärt, was MDM ist. Damit wird für die Beschäftigten klar, was unter diesem Begriff zu verstehen ist. Daraufhin wird der Zweck bestimmt und der Inhalt kurz beschrieben.

> „Das Mobile Device Management (MDM) ist die zentralisierte Verwaltung und Inventarisierung von mobilen Endgeräten (zur Zeit Smartphones und Tablet-PCs) im Unternehmen. Zweck eines MDM ist es, bei gleichzeitigem Schutz des Unternehmensnetzwerks die Sicherheit und Funktionalität des mobilen Endgerätes und die Einbindung in die sonstige betriebliche Infrastruktur zu gewährleisten."
>
> BERGBAU, 090201/531/2012

Hier wird allein auf den Schutzzweck abgestellt. Die folgende Regelung geht darüber hinaus und zeigt auch die „Kehrseite" der Anwendung: den Zugriff auf die mobilen Endgeräte. Damit können die Beschäftigten erkennen, dass sie als Nutzer mobiler Geräte auch persönlich betroffen sind.

> „Bei […] handelt es sich um eine Software-Anwendung zur Verwaltung von mobilen Endgeräten (im Folgenden auch ‚Mobile Devices' genannt). Die Verwaltung umfasst die Einrichtung, die Überwachung und den Support der mobilen Endgeräte. Damit verbunden ist der Zugriff auf ausgewählte Informationen bzgl. der Nutzung der mobilen Endgeräte."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Diese Beispiele zeigen, dass das in den Vereinbarungen verwendete Fachvokabular komplex und damit schwer verständlich wirkt. Die Aufgabe der Betriebsparteien besteht nun insbesondere darin, die Beschäftigten „mitzunehmen" und die Begriffe einfach zu erklären.

2.1 Begriffsbestimmungen

Sofern noch keine Zweckbestimmung erfolgt ist, gilt es zunächst zu erläutern: Was ist ein Mobile Device Managementsystem? Was kann es? Was ist sein Sinn und Zweck? Bei einem MDM handelt es sich um Verwaltungssystem für mobile Endgeräte wie Smartphones und Tablets.

> „Unter mobilen Endgeräten werden Smartphones, IT-Geräte und Tablet-PCs gefasst:
> - Smartphone → Handy mit Internetzugang
> - IT-Gerät → Notebook oder tragbarer Computer mit Internetzugang
> - Tablet-PC."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

MDM verwaltet die Geräte, auf ihnen gespeicherte Daten sowie ihre Möglichkeiten, auf die Unternehmensdaten zuzugreifen, diese abzurufen und zu bearbeiten. Können nur E-Mails abgerufen werden, ist das lediglich eine von vielen Funktionen. Daher stellt sich bei nachfolgender Formulierung die Frage: Sollen andere MDM-Funktionen abgeschaltet werden?

„Um mobile Endgeräte (z. B. Smartphones, [Firma], Tablets) zu verwalten und gesichert bereitzustellen, wird ein Mobile Device Management (MDM) genutzt. Das MDM bietet für diese Endgeräte einen mobilen und drahtlosen Zugriff auf Inhalte des E-Mail-Postfachs bei [der Firma]."

NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Da es neben E-Mail andere Kommunikationswege in den Unternehmen gibt, dient MDM auch dazu, diese Kommunikationsmöglichkeiten zusammenzuführen: Ein Fax landet dann als E-Mail auf dem mobilen Gerät und wird auch über MDM verwaltet.

„Medienübergreifende Zusammenführung der Kommunikationswege und -arten auf ein Endgerät (z. B. Fax to E-Mail)."

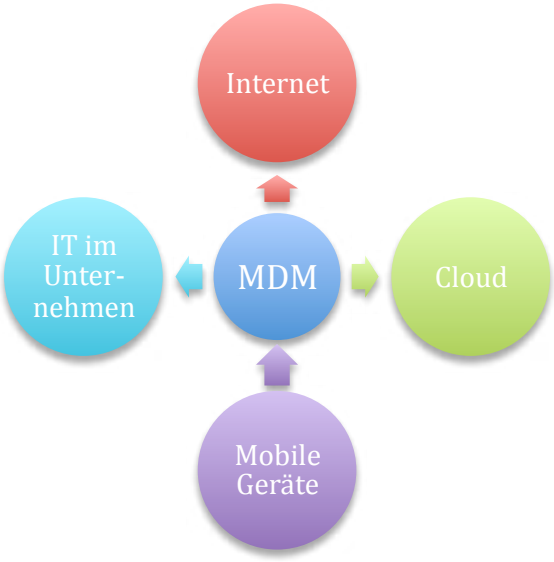
BERGBAU, 090201/531/2012

Kann auf die IT-Systeme des Unternehmens zugegriffen werden, dann ermöglicht es MDM, beliebige Unternehmensdokumente auf den mobilen Endgeräten anzuzeigen. Meist werden die Dateien nicht auf dem mobilen Endgerät gespeichert, sondern vom Server des Unternehmens nur in den temporären Speicher des Gerätes geladen. Sobald die Verbindung des MDM-Systems zum File-Server beendet oder unterbrochen ist, werden alle Daten des geladenen Dokumentes sofort aus dem temporären Speicher gelöscht. MDM ist kein intern geschütztes und abgekapseltes System.

„Durchführen von Zugriffen auf konzerninterne IT-Systeme von außerhalb der Konzern- bzw. Unternehmensinfrastruktur."

BERGBAU, 090201/531/2012

MDM betrachtet auch die Sicherheit hinsichtlich der Internetnutzung. Es werden Schutzfunktionen eingebaut, die ein Ausspähen von Unternehmensdaten verhindern sollen.
In der folgenden Begriffsbestimmung wird MDM als Datenerfassungssystem beschrieben. Die Nutzerinnen und Nutzer können die verschiedensten Funktionen mit den mobilen Geräten über MDM anwenden. Aber: Die Nutzung von Dokumenten durch Anwender wird aufgezeichnet – sowohl ihre Reihenfolge als auch ihre Art und Dauer. Schnittstellen ermöglichen die Weitergabe an beliebige andere Systeme. Hier wird der weite Nutzungsbereich deutlich, der hinsichtlich denkbarer Leistungs- und Verhaltenskontrollen eingeschränkt werden sollte.



Quelle: eigene Darstellung

„Des Weiteren ermöglicht das Datenerfassungssystem den Zugang zu Internet, Datenabgleich mit verschiedenen Office- und Multimediaanwendungen, Installation von Zusatzsoftware (Apps), Videofunktion, Versenden und Empfangen von Mails sowie die Möglichkeit zu telefonieren und zu fotografieren."

ÖFFENTLICHE VERWALTUNG, 090202/199/2012

MDM bietet auch eine Compliance (→ Glossar) für die mobilen Geräte, indem die Einhaltung der Regeln, Grundsätze und Richtlinien des Unternehmens und vor allem des Datenschutzes für die Geräte sichergestellt werden. Beispielsweise lassen sich per Remote-Zugriff die Daten des mobilen Gerätes bei Verlust oder Diebstahl über MDM sofort löschen. Dies gewährleistet die Sicherheit vor Zugriffen Unberechtigter und damit den Datenschutz. Wird dieser Schutz durch einen Jailbreak (→ Glossar) umgangen, erkennt die MDM-Software dies und reagiert entsprechend.

„Die Compliance (Konformität) der Endgeräte wird überprüft. Eines der größten Sicherheitsprobleme ist das sogenannte Jailbreak. Dadurch verliert das Endgerät nicht nur sämtliche Herstellergarantien, sondern auch die eingebauten Sicherheitsfunktionen können dadurch sehr leicht umgangen /deaktiviert werden."

NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Der Begriff Netz wird meist sehr unbedarft für das Internet oder Firmenintranet verwendet. Tatsächlich ist der Begriff jedoch weit vielschichtiger, wie die nachfolgende Regelung zeigt. Man kann nur hoffen, dass die englischsprachigen Begriffe in einem Anhang zur Vereinbarung erklärt werden.

„Netz ist der Oberbegriff für alle Formen der Rechner-Rechner- bzw. Rechner-Telefongeräte-Kopplung (Local Area Network (U\N), Wide Area Network (WAN), Intranet, Internet etc.) unabhängig von deren Topologie und einschließlich aller darin zur Netzsicherheit (A § 8) und zur Netzadministration (A § 9) eingesetzter Hard- und Software (Netz-Management- Systeme, Firewalls, Zugangssicherungssysteme etc.)."

KREDITGEWERBE, 090202/220/2012

2.2 Hardware und Software

MDM verwaltet mobile Geräte und deren Software. Dies kann ausschließlich betriebliche, aber auch private Geräte, Software und Daten betreffen. MDM-Systeme sind in der Regel problemlos in der Lage, alle möglichen Geräte und Systeme zu verwalten. Die Frage ist: Möchte das Unternehmen private Geräte zur beruflichen Nutzung zulassen? Wenn ja: In welchem Umfang?

„Mobiles Arbeiten kann insbesondere mit mobilen Endgeräten wie Laptop oder Smartphone erfolgen. Dabei können sich die mobilen Endgeräte entweder im Eigentum der Firma (sog. ‚Company owned Devices – CoD') oder im Eigentum des Beschäftigten (sog. ‚User owned Devices – UoD') befinden. Entsprechende Festlegungen zur Zulässigkeit der Nutzung von UoD erfolgen durch die Firma."

FAHRZEUGHERSTELLER KRAFTWAGEN, 080102/224/2013

Der Arbeitgeber scheint hier davon auszugehen, alleine festzulegen, welche privaten Geräte wie genutzt werden dürfen. Eine Beteiligung des Betriebsrates erfolgt somit nicht mehr. Der Betriebsrat hat aber ein Beteiligungsrecht bei Festlegung der beruflichen Nutzung privater

Geräte. Denn es handelt sich um eine Regel zum Verhalten und zur Ordnung im Betrieb, die gemäß § 87 Abs. 1 Nr. 1 BetrVG der Mitbestimmung unterliegt (vgl. Kap. 3.1).

2.2.1 Dienstliche Hard- und Software

Die Verwaltung durch MDM zielt darauf ab, den Schutz der Firmendaten auf den mobilen Geräten zu erhöhen. Wo befinden sich welche Daten? Wer hat Zugriff auf welche Daten genommen? Diese Informationen sind für die Unternehmen wichtig. Dafür werden die Geräte in bestimmter Art und Weise konfiguriert und geschützt. Dieser Schutz soll durch die Anwenderinnen und Anwender nicht aufgehoben werden dürfen. Worum es sich jedoch bei einem „Provisioning-Zertifikat“ (→ Glossar) handelt, erschließt sich sicher nicht jedem sofort. Wer schon einmal ein Elektroauto an einer öffentlichen Ladestation aufgeladen hat, kennt ein „Certificate Provisioning“ – eine Zertifikatsbereitstellung. Damit „tauschen“ sich Auto und Ladestation „aus“ und alle nötigen Daten für die richtige Ladung, aber auch für die Abrechnung der Kosten werden übertragen. Für MDM bedeutet dies: Nur dieses bestimmte Gerät darf Daten des Unternehmens abrufen und aufnehmen.

> „Alle durch [die Firma] bereitgestellten mobilen Geräte, die auf Firmendaten und -systeme Zugriff haben, werden durch die Mobile Device Management-Lösung (MDM) der jeweiligen IT-Abteilung verwaltet. Die Entfernung von Provisioning- und Konfigurationszertifikaten ist nicht zulässig.“
>
> CHEMISCHE INDUSTRIE, 090202/190/2012

Laut nachfolgender Regelung ermöglicht es das MDM, die unternehmensinternen Sicherheitsrichtlinien einzuhalten. Vollständigkeitshalber wäre hinzuzufügen: Auch die Kontrolle, ob die Richtlinien eingehalten werden, wird ebenso bzw. nur durch MDM möglich.

> „Das Mobile Device Management ermöglicht die Einhaltung von Sicherheitsrichtlinien, sowie die interne Verteilung und Administration von Applikationen.“
>
> CHEMISCHE INDUSTRIE, 050340/39/2012

Die Kontrolle beginnt bei der Frage: Welche Apps (Programme) dürfen genutzt werden? Ein Weg ist die sogenannte Black-List: die Beschreibung, was alles nicht genutzt werden darf. Das ist sicher für Nutzer der klarere Weg, wenn die Liste übersichtlich ist. Vermutlich ist die Liste aber aufgrund der Vielzahl von Apps nicht kurz und übersichtlich – und damit schnell unüberschaubar. Dann wäre eine „White-List“ einfacher einzuhalten: Geladen werden darf alles, was sich auf dieser Liste befindet oder ausdrücklich genehmigt wurde. In beiden Fällen ist es jedoch erforderlich, die Listen ständig zu aktualisieren.

> „Die Liste der aktuell nicht zugelassenen Applikationen (Black-List) wird jeweils aktuell im [Intranet] bereitgestellt.“
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

> „Das Herunterladen von in dieser White-List nicht enthaltenen Apps bedarf der vorherigen Genehmigung durch den Arbeitgeber. In jedem Falle ist das Herunterladen von Spielen und sämtlichen Apps mit pornografischem oder extremistischen Inhalten ausnahmslos verboten.“
>
> LEASINGUNTERNEHMEN, 090202/196/2012

2.2.2 Private Geräte (BYOD)

Die Zulassung privater Geräte wird unterschiedlich gehandhabt (Bring your own device, → Glossar). Manche Unternehmen lassen jedes Gerät zu und treffen nur bezüglich der Software eine Auswahl.

> „Allen Mitarbeitern werden auf Antrag der dienstliche [Firma] Notes Kalender und die persönlichen [Firma] Notes Kontakte auf ihrem privaten Endgerät zur Verfügung gestellt."
>
> VERSICHERUNGSGEWERBE, 090202/206/2014

Anderen Unternehmen ist es wichtiger, die zulässige Hardware einzugrenzen – wahrscheinlich, um sich nicht mit unzähligen Varianten und diversen Betriebssystemen beschäftigen zu müssen. Im Folgenden legt sich der Arbeitgeber auf iOS-Produkte (→ Glossar) fest, lässt also nur Apple-Geräte zu.

> „Diese Vereinbarung regelt die Möglichkeit einer Nutzung der von der [Firma] zur Verfügung gestellten Applikationen mit Hilfe privater Smartphones/Tablets (private Hardware). Hierbei ist die Auswahl beschränkt auf die von der [Firma] freigegebenen Gerätetypen ([Firma] Hardware mit iOS, die in der Lage sind, mit der jeweils aktuellsten Firmware zu arbeiten)."
>
> VERSICHERUNGSGEWERBE, 090202/206/2014

In der nachstehenden Vereinbarung bleibt offen, nach welchen Kriterien das Unternehmen private Geräte und die private Nutzung zulässt. Klar ist nur: Die Beschäftigten haben keinen Anspruch auf Zulassung ihres Gerätes.

> „Die Beschäftigten haben weder einen Anspruch auf die dienstliche Nutzung eines privaten IT-Systems noch auf die Einrichtung oder Zulassung einer vorübergehenden oder dauerhaften Verbindung eines privaten mit einem dienstlichen IT-System. Die Konzerngesellschaften können hiervon abweichende Regelungen treffen."
>
> BERGBAU, 090201/531/2012

Nicht den Wünschen der Beschäftigten entsprechen dürfte die Regelung, die nur die dienstliche Telefonie mit den privaten mobilen Geräten zulässt. Da stellt sich die Frage: Müssen die Beschäftigten sich in diesem Fall überhaupt bei MDM anmelden? Denn es darf ja kein Datenverkehr stattfinden. Müssen sie ihr Gerät nicht anmelden, dann kann das Unternehmen nicht kontrollieren, ob die nachstehende Regelung eingehalten wird. Übernimmt das Unternehmen keine Kosten für dienstliche Gespräche, ist eine Pflicht zur Anmeldung von privaten Geräten bei MDM nicht erkennbar.

> „Eine Nutzung privater Endgeräte für betriebliche Belange ist weiterhin generell auf Wunsch des Mitarbeiters möglich, allerdings beschränkt sich dies auf reine Telefonie."
>
> LANDVERKEHR, 090202/197/2013

Den optimalen Schutz der privaten Daten gewährleistet die nachstehende Bestimmung, indem sie eine dienstliche Nutzung ausschließt. Die Wünsche der Beschäftigten sehen in der Praxis jedoch häufig anders aus. Sie möchten kein zweites, dienstliches Smartphone mit sich herumtragen müssen, wenn ihr privates gleichermaßen alle Funktionen erfüllt.

> „Private mobile Endgeräte der Beschäftigten werden nicht über das MDM-System erfasst. Sie dürfen nicht dienstlich genutzt werden und können keinen Zugriff auf das Firmennetzwerk herstellen."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

2.2.3 Private Apps

Im privaten Bereich ein Smartphone zu nutzen, ist heute für die meisten Beschäftigten eine Selbstverständlichkeit. Bestimmte Apps würden viele gern auch auf dem dienstlichen Gerät anwenden: sei es die Wetter-App, die App für die regionale Tageszeitung oder Facebook. Um keine Sicherheitsrisiken einzugehen, schließen einige Unternehmen die Nutzung privater Apps aus.

> „Der Mitarbeiter ist nicht befugt, weitere Apps auf das Gerät ohne vorherige Zustimmung der Gesellschaften zu laden."
>
> GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Einen anderen Weg wählt folgende Regelung. Sie lässt die Nutzung privat installierter Apps grundsätzlich zu. Allerdings verlagert sie die Verantwortung auf die Beschäftigten, indem sie empfiehlt, nur „sichere Apps" zu laden. Was aber unterscheidet eine sichere von einer unsicheren App? Dies wird nur mit dem Hinweis beantwortet, dass manche Apps angeblich Adressbücher auslesen oder Daten sammeln. Herauszufinden, welche Apps konkret gemeint sein könnten, obliegt den Beschäftigten selbst.

> „Die Installation von Fremdapplikationen, auch für die private Nutzung, ist gestattet. Die Kosten für Fremdapplikationen für den Privatgebrauch sind von dem Mitarbeiter zu tragen. Einige Applikationen stehen im Verdacht, Daten zu sammeln oder z. B. Adressbücher auszulesen. Das Unternehmen empfiehlt, auch im Interesse des Mitarbeiters, darauf zu achten, dass nur sichere Applikationen genutzt werden."
>
> FAHRZEUGHERSTELLER KRAFTWAGEN, 090202/203/0

Nachstehend ermöglichen die Betriebsparteien indirekt, dass eine private Nutzung jederzeit wieder untersagt werden darf, wenn der Einsatz des Gerätes für betriebliche Belange gefährdet wird. Die Anwender sollen für die Einsatzfähigkeit „Sorge tragen" und auch Apps daraufhin prüfen. Was konkret gemeint ist und wo welche Gefährdungen liegen könnten, bleibt unklar.

> „Die private Nutzung unterliegt dem Vorbehalt, dass der Nutzer Sorge trägt für die Einsetzbarkeit des Gerätes für seine betrieblichen Belange, soweit er darauf Einfluss nehmen kann. Insbesondere eine Installation von Apps und anderer Software ist vom Nutzer nach besten Wissen und Gewissen darauf zu überprüfen."
>
> LANDVERKEHR, 090202/197/2013

Völlig freigestellt wird die Nutzung von Apps im Folgenden. Allerdings sind erneut die Beschäftigten dafür verantwortlich, dass alle Schutz- und Sicherheitsregeln eingehalten werden. Das dürfte für die meisten schwer realisierbar sein. Denn viele Anwendungen stellen im Hintergrund Verknüpfungen her, rufen Daten ab und nutzen sie auf dem mobilen Gerät, ohne zu fragen oder das sichtbar zu machen.

> „Anwendungen für iPads, die online über einen Dritten bezogen werden können (sog. Apps), können zu privaten Zwecken installiert werden, sofern der Mitarbeiter die Regelungen dieser Betriebsvereinbarung beachtet, insbesondere die Ziffern 4.2 und 6.3. Der Mitarbeiter kann – sofern er dies wünscht – die GPS-Funktion [→ Glossar] zur Nutzung von Apps aktivieren."
>
> CHEMISCHE INDUSTRIE, 050340/39/2012

Die nachstehende Regelung aus den Nutzungsbedingungen für das iPhone zeigt exemplarisch: Es ist schwierig zu erkennen, was die Anwendungen auf den Geräten alles leisten können.

„Sie erklären ihr Einverständnis damit, dass Apple, seine Tochtergesellschaften und Auftragnehmer Diagnosedaten sowie technische Informationen, Nutzungsdaten und zugehörige Informationen, einschließlich insbesondere Informationen über ihr iPhone, ihren Computer, Ihre Systemsoftware und Softwareprogramme sowie Peripheriegeräte sammeln, verwalten, verarbeiten und verwenden dürfen, sofern diese für die iPhone Software relevant sind."

(HTTP://IMAGES.APPLE.COM/LEGAL/SLA/DOCS/IOS81.PDF)

2.3 Nutzungsmöglichkeiten

In Kap. 2.2 wurde beschrieben, welche Hard- und Software zum Einsatz kommen darf und welche privaten Geräte oder Apps erlaubt sind. In manchen Vereinbarungen wird im nächsten Schritt die Nutzung differenzierter betrachtet und in der Regel eingeschränkt.

2.3.1 Dienstliche Nutzung

Aus Sicht des Unternehmens ist es sinnvoll, die Nutzungsmöglichkeiten der Software zu beschreiben. Damit wird festgelegt, welche Anwendungen mitbestimmungspflichtig und seitens des Unternehmens zulässig sind.

„Das MDM umfasst folgende Prozesse und Dienste bzw. stellt diese bereit:
- Inventarisierung und Aktivierung einsatzbereiter mobiler Endgeräte
- Ausrollen und Management von Sicherheits-Richtlinien auf mobilen Endgeräten
- Ausrollen und Management von Anwendungen
- Ausrollen von Softwareaktualisierungen (z. B. des Betriebssystems und der Anwendungen)
- Löschen der dienstlichen Daten aus der Ferne (z. B. bei Verlust)
- Management und Synchronisation des Datenverkehr zwischen mobilen Endgeräten und Unternehmensanwendungen."

BERGBAU, 090201/531/2012

Auch aus Sicht des Datenschutzes ist die Zweckbestimmung besonders relevant. Denn die Betriebsvereinbarung kann die rechtliche Basis für datenschutzrechtlich zulässige Nutzungen darstellen (vgl. Kap. 2.6 und 3.4).

„[Die Firma] wird in der Mediengruppe [der Firma] zu folgenden Zwecken eingesetzt: [...]
- Management der verpflichtend Installierten und der nicht zugelassenen Apps
- Überwachung der Einhaltung der Sicherheitsstandards gemäß dieser Konzernbetriebsvereinbarung bei der Nutzung von mobilen Endgeräten
- Überwachung der Einhaltung des Datenschutzes gemäß dieser Konzernbetriebsvereinbarung bei der Nutzung von mobilen Endgeräten."

VERLAGS- UND DRUCKGEWERB , 090202/209/2013

Wie immer im IT-Bereich ist es sinnvoll, die Nutzungsmöglichkeiten auch für MDM zu beschränken. Eine Positivbeschreibung deklariert, was die Software ausschließlich leisten darf. Alle anderen Funktionen sind unzulässig. Entsprechende Daten dürfen nicht gewonnen und schon gar nicht zum Nachteil der Beschäftigten verwendet werden.

„Die […]-Anwendung wird ausschließlich für folgende Zwecke genutzt: [...]
- automatisierte Überprüfung der auf dem Smartphone installierten Apps in Bezug auf Malware (Viren, Trojaner etc.); im positiven Fall wird der System-Administrator umgehend darüber informiert.
- Zurücksetzen des Smartphones auf Werkseinstellungen und/oder Löschen des Datencontainers für die geschäftlichen Daten durch den Besitzer des Smartphones oder den Smartphone-Administrator."

LEASINGUNTERNEHMEN, 090202/196/2012

Um nicht bei jeder erforderlichen Ergänzung der Nutzungsmöglichkeiten die Betriebsvereinbarung ändern zu müssen, kann ein Zustimmungsvorbehalt für Erweiterungen sinnvoll sein. Dabei stellt sich nur die Frage: Wo wird dies – auch für die Beschäftigten nachvollziehbar – dokumentiert?

„Weitere Einsatzzwecke bedürfen der Zustimmung des BR."

LEASINGUNTERNEHMEN, 090202/196/2012

2.3.2 Privatnutzung

Werden dienstliche Geräte zur privaten Nutzung zugelassen, gilt es zu klären, in welchem Umfang und welche Geräte konkret genutzt werden dürfen. Eine unbeschränkte und unentgeltliche Privatnutzung erlaubt die folgende Regelung.

„Die von der [Firma] zur Verfügung gestellten Smartphones und Tablet-PCs dürfen außerhalb des Betriebes und der Arbeitszeiten von den Beschäftigten zeitlich unbegrenzt und unentgeltlich privat genutzt werden. Das heißt, es können insbesondere Telefonate geführt, Kurzmitteilungen verschickt und private Daten, wie etwa Fotodateien, gespeichert werden. Die Beschäftigten sind ebenfalls dazu berechtigt, private Emails zu versenden und zu empfangen sowie Apps zum privaten Gebrauch herunterzuladen."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Da erhebliche Mehrkosten entstehen können durch die Nutzung mobiler Geräte im Ausland, schließt die nachfolgende Regelung dies aus. Eine unbeschränkte Privatnutzung ist danach nur im Inland zulässig. Ausgeschlossen wird auch eine Nutzung durch Dritte, die nicht dem Unternehmen angehören.

„Die Privatnutzung ist ausschließlich dem Mitarbeiter gestattet. Das iPad und/oder das dazugehörige Passwort darf nicht an nicht-unternehmensangehörige Dritte weitergegeben werden. Die Privatnutzung im Ausland ist dem Mitarbeiter nicht gestattet."

CHEMISCHE INDUSTRIE, 050340/39/2012

Im Folgenden geht es insbesondere darum, bestehende Regeln für die Nutzung dienstlicher E-Mail-Accounts nicht durch mobile Geräte aufzuweichen. Daher ist es nur eingeschränkt zulässig, den dienstlichen Account privat zu nutzen.

„Für E-Mails gilt, dass es dem Arbeitnehmer gestattet ist, einen privaten eMail-Account über das iPad abzurufen. Für die Nutzung des dienstlichen eMail-Accounts (dienstliche und private eMails) gelten die Regelungen der Gesamtbetriebsvereinbarung Elektronische Kommunikationsdienste vom 10.08.2007."

CHEMISCHE INDUSTRIE, 050340/39/2012

Nutzungsbeschränkungen für die Beschäftigten sollten möglichst keine unbestimmten Begriffe enthalten. Die folgende Regelung wirft beispielsweise die Frage auf: Was genau könnte mit dem „verantwortlichen Rahmen“ und den „betrieblichen Belangen“ gemeint sein?

> „Eine private Nutzung der Endgeräte ist zulässig, soweit sie im verantwortlichen Rahmen erfolgt und betriebliche Belange nicht beeinträchtigt werden; für diesen Fall gibt sie keinen Anlass zu arbeitsrechtlichen Maßnahmen (Sanktionen).“
>
> KREDITGEWERBE, 090202/220/2012

Ein weiteres Beispiel: Welche Interessen eines Unternehmens sind berechtigt, welche nicht? Die folgende Regelung findet dafür einige Beispiele, schränkt die Aufzählung aber durch den Zusatz „insbesondere“ ein. Konkreteres erfahren die Beschäftigten nicht: Zwar werden einige Gesetze benannt, deren Inhalt dürften die Beschäftigten jedoch nicht kennen.

> „Unzulässig ist jedoch jede Nutzung des Internets, die potenziell dazu geeignet ist, berechtigte Interessen der Unternehmen zu beeinträchtigen oder die Unternehmen in ihrem öffentlichen Ruf zu schädigen. Insbesondere ist den Mitarbeitern das Aufrufen, Abrufen, Herunterladen oder Verbreiten von Inhalten verboten, die gegen persönlichkeits-, datenschutz-, urheber- oder strafrechtliche Bestimmungen verstoßen oder beleidigender, verleumderischer, rassistischer, sexistischer, pornografischer, gewaltverherrlichender oder verfassungsfeindlicher Art sind.“
>
> GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Der Versuch, mit unbestimmten Begriffen einen möglichst weiten Verbotsrahmen zu ziehen, schlägt fehl. Was genau umfassen beispielsweise „persönlichkeitsrechtliche Bestimmungen“? Wo ist dies nachzulesen? Welche Beispiele gibt es dafür? So lange diese Fragen ungeklärt sind, führen sie nicht zu wirksamen Regelungen – sondern bleiben unbestimmt, intransparent und für arbeitsrechtliche Sanktionen ungeeignet.
Die Betriebsparteien sollten nicht davon ausgehen, dass alle Beschäftigten die IT-Sprache verstehen. Idealerweise werden, wie im folgenden Beispiel, englischsprachige Wörter kurz in Deutsch erklärt.

> „Die Nutzung von Cloud-Diensten (Speicherung von Daten bei Drittanbietern) ist den Mitarbeitern ausnahmslos untersagt.“
>
> LEASINGUNTERNEHMEN, 090202/196/2012

Sicherlich beabsichtigten die Betriebsparteien mit der folgenden Bestimmung, die privaten Daten zu schützen. Allerdings wird hierdurch nicht geregelt, dass dem Arbeitgeber die Einsichtnahme am Arbeitsplatz verboten wäre. Es würde sich anbieten, ihm die Kontrolle der privaten Ordner zu untersagen.

> „Private Daten und Dateien dürfen ausschließlich auf bzw. in hierfür eingerichteten und als solche gekennzeichneten Laufwerken und Ordnern gespeichert werden.“
>
> KREDITGEWERBE, 090202/220/2012

2.3.3 Passwortschutz

Die MDM-Systeme werden gern wie eine Mauer zwischen den mobilen Geräten und den Unternehmensdaten bzw. -servern dargestellt. Zugriff auf Daten des Unternehmens haben nur Geräte, die durch MDM autorisiert sind. Häufig sind die Unternehmensdaten in einer Art Safe auf dem mobilen Gerät gespeichert. Jeder Zugriff erfordert von den Nutzern, dass sie sich

als Berechtigte mittels eines Passwortes ausweisen. Laut nachfolgender Regelung muss zudem das Passwort in regelmäßigen Abständen erneuert werden.

> „Benutzer melden sich zu den Systemen und Anwendungen der Bank mit einer eindeutigen Benutzerkennung und einem persönlichen Passwort an; das Passwort muss in regelmäßigen Abständen geändert werden. Die Autorisierung für die eingesetzten Systeme ist Aufgabe der Bank."
>
> KREDITGEWERBE, 090202/220/2012

Die Passwörter müssen zudem bestimmten Standards genügen, um zu verhindern, dass Unbefugte sie entschlüsseln. Dies erfordert durchaus Fantasie von den Beschäftigten: Sie müssen sich regelmäßig neue und sichere Passwörter ausdenken und dürfen diese nicht vergessen – ohne sie zu notieren.

> „Der Zugriff auf die mobilen Endgeräte wird durch die zwingende Einrichtung eines persönlichen Passwortes abgesichert. Das Passwort hat den Anforderungen der Sicherheitsstandards des Betriebskonzeptes (Anlage 1, Abschnitt 4.4) zu genügen."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Einerseits ist es für die Beschäftigten komfortabler, wenn laut Regelung die Administratoren die Passwörter festlegen; andererseits müssen sie sich die fremden Zeichenreihen irgendwie merken. Da die Passwörter selbstverständlich geheim gehalten werden müssen, dürfen sie nirgendwo notiert werden.

> „Jeder Programmnutzer/Gerätenutzer erhält von den zuständigen Administratoren ein persönliches Passwort, das bei jedem Aufruf des Programms/Nutzung des Gerätes durch den Nutzer automatisch abgefragt wird. Ohne Eingabe der PIN/des Passwortes ist die Nutzung nicht möglich. Die Passwortanforderungen werden entsprechend dem Datenschutzkonzept festgelegt. Die PIN bzw. das Passwort sind vom Nutzer geheim zu halten; ihre Weitergabe ist untersagt. Voreinstellungen des Gerätes sind insofern nicht zu verändern."
>
> BILDUNGSEINRICHTUNG, 090202/198/2013

Es bleibt zu hoffen, dass die bei iOS-Geräten neuerdings genutzten Fingerscanner auch für komplizierte Passwörter genutzt werden können und die Neuvergabe bzw. das Einprägen von fremden Passwörtern bald der Vergangenheit angehört.

2.3.4 Nutzungsbestimmungen

Neben der Frage, ob eine Nutzung überhaupt zulässig ist, kann zudem die Art und Weise der Nutzung geregelt werden. Die nachfolgende Vereinbarung stellt es den Beschäftigten anheim, eines von zwei Verschlüsselungsverfahren anzuwenden – scheinbar eine Möglichkeit, um einerseits unterschiedliche private Geräte zu nutzen und andererseits den verschlüsselten Datenverkehr zu sichern.

> „Eine Verschlüsselung, z. B. gemäß dem Advanced Encryption Standard (AES) oder dem Data Encryption Standard (DES), ist sowohl auf dem Gerät als auch bei den Sicherungen des Gerätes anzuwenden. Sie wird durch das MDM Provisioning-Zertifikat der betreffenden IT-Abteilung verwaltet."
>
> CHEMISCHE INDUSTRIE, 090202/190/2012

Zur mobilen Nutzung gehört unter Umständen auch, dass mit dem mobilen Gerät empfangene oder eingegebene Daten mittels MDM auf den Servern des Unternehmens gespeichert werden. Leicht wäre es möglich, auch andere Speicherdienste und -orte zu verwenden. Doch genau dies soll verhindert werden, um die unternehmensinternen Informationen schützen.

> „Erfolgt die Speicherung von unternehmensbezogenen Daten auf Servern, so darf dies nur auf firmeneigenen Servern erfolgen. Eine Ablage der Daten auf Filesharing-Servern, wie zum Beispiel Dropbox oder iCloud, ist nicht gestattet."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

In der Regel müssen die Beschäftigten die Daten auf ihren mobilen Geräten vor Zugriffen Dritter schützen. Idealerweise wird in der Vereinbarung erklärt, welche Maßnahmen das Unternehmen konkret erwartet.

> „Darüber hinaus hat der Mitarbeiter sicherzustellen, dass das Mobile Device, alle sich darauf befindlichen geschäftsrelevanten Daten sowie alle Daten von zentralen Ablagestrukturen, auf welche mit Hilfe des Mobile Device zugegriffen werden kann, vor fremden Zugriffen geschützt sind. Das Gerätekennwort, die PIN-Funktion oder SIM-Karte und [die Anwendung für MDM] – dürfen zu keinem Zeitpunkt deaktiviert werden."
>
> FAHRZEUGHERSTELLER KRAFTWAGEN, 090202/203/0

Alle Nutzerinnen und Nutzer von IT-Technik wissen, wie wichtig eine aktuelle Schutzsoftware ist. Aber warum sind laut folgender Bestimmung die Beschäftigten dafür zuständig, die Geräte auf dem aktuellen Stand zu halten? Wie erfahren sie von Updates? Eine wichtige Funktion von MDM besteht doch insbesondere darin, ein Update von außen zu ermöglichen.

> „Der Nutzer verpflichtet sich, die für das jeweilige Gerät aktuellste und durch das [Firmen-]Rechenzentrum für den Einsatz in der Mediengruppe […] freigegebene Betriebssystemsoftware auf dem mobilen Endgerät zu installieren."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Bei einigen Systemen ist es möglich, alle Daten des geladenen Dokumentes sofort aus dem temporären Speicher zu löschen, falls die Verbindung vom MDM-System zum File-Server beendet oder unterbrochen wird. Bei Verlust oder Diebstahl des mobilen Endgerätes können somit Dokumente des Unternehmens nicht in die Hände Unberechtigter gelangen. Zudem wird sichergestellt, dass nicht einmal Spuren von Daten auf dem mobilen Gerät verbleiben. Bei anderen Systemen werden per Remote-Zugriff die Daten des mobilen Gerätes bei Verlust oder Diebstahl sofort gelöscht und damit der Datenschutz sowie die Sicherheit vor Zugriffen Unberechtigter auf interne Informationen gewährleistet. Wurden private Apps nach der Installation von MDM aufgespielt, sind diese und die dazugehörigen Daten bei einer „Fernlöschung" ebenso verloren. Darauf verweist die nachfolgende Regelung. Es bleibt zu hoffen, dass die Beschäftigten ein privates Backup ihrer Daten erstellen.

> „Ich verpflichte mich zur Einhaltung der Nutzungsbestimmungen für das mobile Endgerät und erkläre mich damit einverstanden, dass mein mobiles Endgerät über die Mobile Device Management-Software [Firma] administriert und bei Verlust administrativ gelöscht werden wird. Eine Abschrift dieser Nutzungsbestimmungen habe ich erhalten."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

2.4 Arbeitszeit/Bereitschaftsregelungen

Neben der elektronischen Post und dem Kalender sind auch Arbeitsanweisungen, Anleitungen und beispielsweise Betriebsvereinbarungen auf dem Tablet oder Smartphone stets zur Hand und einsehbar. Über MDM ist der Zugriff auf Unternehmensdaten von jedem Ort zu jeder Zeit grundsätzlich möglich. Daher eignet sich eine Betriebsvereinbarung zum MDM auch dazu, Arbeitszeitfragen zu regeln. Eine klare Abgrenzung zwischen Arbeitszeit und Freizeit ist in der folgenden Regelung nicht sofort erkennbar. Möglicherweise ist sie in der betrieblichen Arbeitszeitregelung enthalten.

> „Auch bei der Nutzung von mobilen Endgeräten sind die gesetzlichen, tariflichen und die örtlich mit dem Betriebsrat vereinbarten Arbeitszeitregelungen einzuhalten."
>
> FAHRZEUGHERSTELLER KRAFTWAGEN, 080102/224/2013

Klarer und sofort nachvollziehbar ist das Verbot, mit mobilen Geräten außerhalb der bisher üblichen Arbeitszeiten weiterzuarbeiten.

> „Die dienstliche Nutzung der mobilen Endgeräte erfolgt ausschließlich während der üblichen vereinbarten Arbeitszeit. Grundlage bilden die jeweiligen Arbeitsverträge und Tarifverträge."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Mit der folgenden Vereinbarung legen die Betriebsparteien die Verantwortung in die Hände der Beschäftigten: Sie dürfen ihre mobilen Geräte außerhalb der individuellen Arbeitszeit ausschalten. Dies wirft die Frage auf: Soll damit angedeutet werden, dass sie die Geräte ebenso gut anlassen dürfen? Denn das Ausschalten außerhalb der Arbeitszeit ist eine Selbstverständlichkeit.

> „Die Beschäftigten sind berechtigt, ihre mobilen Endgeräte außerhalb der individuellen Arbeitszeit auszuschalten."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Lassen die Beschäftigten außerhalb der Arbeitszeit die dienstlichen mobilen Geräte angeschaltet und beantworten dienstliche Mails, stellt sich schnell die Frage nach der Bezahlung von Arbeitszeit. Die folgende Regelung soll vor einer ausufernden Entgeltpflicht schützen. Die Grundregel im Arbeitsverhältnis lautet jedoch: Der Arbeitgeber muss die Arbeit, die er entgegennimmt, auch bezahlen (vgl. Kap. 3.2). Daher ist die nachfolgende Regelung mit dem Ausschluss der Anrechnung von Arbeitszeit unklar und unwirksam.

> „Besitz oder Nutzung des Tokens begründen für sich keinen Anspruch auf Anrechnung als Arbeitszeit. Die Frage, ob die Zeiten der Nutzung des Tokens als Dienst- oder Arbeitszeit zu bewerten sind, richtet sich nach der Dienstvereinbarung über die Regelung der täglichen Arbeitszeit. Die Nutzung außerhalb der Kernarbeitszeit beruht grundsätzlich auf dem Prinzip der Freiwilligkeit. [...] Die Anrechnung der Arbeitszeit aufgrund dienstlicher Erfordernisse erfolgt in Absprache zwischen der/dem unmittelbaren Vorgesetzten und der/dem Beschäftigten."
>
> ÖFFENTLICHE VERWALTUNG, 080102/223/2013

Gern werden mobile Geräte auch als eine Art Ersatz für Rufbereitschaft angesehen. Dies schließt folgende Vereinbarung aus. Nur weil die Beschäftigten das Smartphone vielleicht auch privat nutzen dürfen, müssen sie nicht ständig für den Arbeitgeber erreichbar sein.

„Die Möglichkeit der Rufbereitschaft/Arbeit auf Abruf ist ausgeschlossen. Eine Kontaktaufnahme zu diesem Zweck kann nicht über das mobile Endgerät hergestellt werden. Vielmehr wäre für Rufbereitschaft/Arbeit auf Abruf eine gesonderte Regelung erforderlich."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Überträgt man die Verantwortung für die dienstliche Nutzung der mobilen Endgeräte außerhalb der Arbeitszeit den Beschäftigten bzw. stellt man die Nutzung unter den Vorbehalt der Freiwilligkeit, birgt dies neben der Frage der Bezahlung von Arbeitszeit zusätzliche Gefahren (vgl. Kap. 3.2).

2.5 Qualifizierungsregelungen

In den Betriebs- und Dienstvereinbarungen finden sich nur wenige Regelungen zur Qualifizierung der Beschäftigten. Die wenigen vorhandenen Regelungen bleiben größtenteils recht allgemein. Es liegt nahe, dass die Nutzung der mobilen Geräte oder eine bestimmte Anwendung meist gelernt werden muss. Zu MDM selbst findet sich jedoch keine einzige konkrete Regelung. Nachfolgend kann es vielleicht noch unter die „vorgesehene Nutzung" gefasst werden.

„Die Mitarbeiter werden vor der erstmaligen Zurverfügungstellung von iPads in geeigneter Weise umfassend in deren Anwendung geschult. Gleiches gilt für die Anwendung von Applikationen. Darüber hinaus wird sichergestellt, dass der Mitarbeiter für die vorgesehene Nutzung eine ausreichende weitere Unterstützung erhält (z. B. Coaching, eLearning, Training, etc.)."

CHEMISCHE INDUSTRIE, 050340/39/2012

Die folgende Bestimmung berücksichtigt: Es bestehen Missbrauchsgefahren und die Beschäftigten müssen hierüber zumindest aufgeklärt werden.

„Alle Beschäftigten werden vor der Nutzung neuer Systeme in Abstimmung mit dem GBR angemessen qualifiziert. Bestandteil dieser Maßnahmen ist u. a. auch die Erläuterung dieser GBV. Insbesondere werden sie auch über Missbrauchsmöglichkeiten und Gefahren […] sowie über Maßnahmen zum Schutz ihrer Persönlichkeitsrechte aufgeklärt."

KREDITGEWERBE, 090202/220/2012

Richtig ist: Nach § 98 BetrVG hat der Betriebsrat hinsichtlich der Durchführung von betrieblichen Qualifizierungsmaßnahmen mitzubestimmen. Aufgrund § 96 BetrVG könnte der Betriebsrat auch Vorschläge zur inhaltlichen Ausgestaltung machen – erzwingen kann er sie jedoch nicht. Daher wäre es sinnvoll, die Inhalte erforderlicher Schulungen in einer Betriebsvereinbarung zu MDM zu konkretisieren. Laut nachstehender Regelung obliegt es dem Arbeitgeber, die erforderlichen Schulungsmaßnahmen auszusuchen.

„Der AG [Arbeitgeber] wird die von der Einführung betroffenen Mitarbeiter im erforderlichen Umfang schulen. Dabei können u. a. auch Schulungen im Rahmen des ‚e-learning' in Betracht kommen. Die möglichen Qualifizierungsmaßnahmen finden während der Arbeitszeit statt. Im Übrigen bleiben die Regelungen des § 98 BetrVG unberührt."

LEASINGUNTERNEHMEN, 090202/196/2012

2.6 Datenschutz

Gemäß vielen Einführungsregelungen zu MDM-Vereinbarungen ist die Sicherheit von Unternehmensdaten ein zentraler Zweck. Die Daten des Unternehmens sollen geschützt werden. Durch mobile Geräte entstehende Sicherheitslücken gilt es zu schließen. Der Leitsatz der folgenden Regelung im Zusammenhang mit der Nutzung von MDM lautet: Gegeneinander abzuwägen sind einerseits die Sicherheit des Unternehmens und seine Interessen (welche? bleibt offen) und andererseits die Bedürfnisse der Beschäftigten (welche? bleibt ebenso offen). Damit wird zumindest indirekt anerkannt: Auch der Schutz der Beschäftigtendaten stellt einen Einsatzzweck von MDM dar.

> „Der Einsatz [der Firma] im Zusammenhang mit den mobilen Endgeräten soll die Sicherheit der Unternehmen der Mediengruppe […] optimieren, wobei die Bedürfnisse der Beschäftigten (dazu gehört auch die Arbeitszufriedenheit) und die Interessen des Mediengruppe […] zu berücksichtigen sind."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Auch der Schutz der privaten Daten der Beschäftigten kann durch MDM gewährleistet werden. Dies ist immer sinnvoll und nötig, wenn private Geräte genutzt werden dürfen oder dienstliche Geräte für private Zwecke. Dieser Bereich muss in mehrfacher Hinsicht geschützt werden: Zum einen vor dem Zugriff durch den Arbeitgeber oder durch nicht autorisierte Kolleginnen und Kollegen; zum anderen vor dem Zugriff durch unberechtigte Dritte. Zudem wäre bei Verlust des Gerätes auch eine Sicherung der privaten Daten sehr hilfreich. In der nachstehenden Regelung wird das Problem des Umgangs mit privaten Daten richtigerweise ausdrücklich als regelungsbedürftig erkannt.

> „Sofern ein Beschäftigter dienstliche IT-Systeme für private Zwecke nutzt, kann eine Kenntnisnahme der privaten Daten oder Informationen durch Dritte nicht ausgeschlossen werden. Vereinbarungen von Konzerngesellschaften, die eine private Nutzung dienstlicher IT-Systeme erlauben, müssen daher auch Regelungen zum Umgang mit privaten Daten und Informationen sowie zu deren Schutz treffen, etwa für den Fall einer längeren Abwesenheit des Beschäftigten oder für das Vorliegen des Verdachts auf eine strafbare Handlung."
>
> BERGBAU, 090201/531/2012

2.6.1 Personenbezogene und andere Daten

Durch MDM können unterschiedlichste Daten erfasst und gespeichert werden. Laut folgender Regelung wird MDM auf eine Schutzfunktion beschränkt und nicht noch zusätzlich als Datenspeicher eingesetzt. Es wird so konfiguriert, dass eine Speicherung nicht möglich ist. Das ist der beste Schutz vor ungewollten Auswertungen.

> „Eine Speicherung von Inhaltsdaten, Telefonaten oder E-Mails einschließlich dazugehöriger Log-Dateien auf dem benötigten Server ist nicht möglich."
>
> BILDUNGSEINRICHTUNG, 090202/198/2013

Einerseits ist es sinnvoll und andererseits wohl nicht zu verhindern, dass Protokolle des Systems erstellt werden. Darin wird beispielsweise aufgezeichnet, wann welches Gerät welche Daten genutzt oder gesendet hat. Da die Geräte bestimmten Personen zugeordnet sind, ist damit auch eine personenbezogene Auswertung möglich. Diese liefert Daten über die Leistung und das Verhalten der Beschäftigten: beispielsweise wann mit dem Gerät gearbeitet wurde (Leistung) oder wann ein privater Datenverkehr stattfand (Verhalten). Die nachstehende Re-

gelung beschreibt diese Möglichkeit. Dazu ist eine weitere Regelung nötig, um Auswertungen zu begrenzen bzw. um sie zuzulassen.

> „Über die Erstellung des Systemprotokolls und eine etwaige Aufzeichnung der Aufschaltungssitzung hinaus werden keine personenbezogenen Daten erhoben, verarbeitet oder genutzt. Es kann jedoch nicht ausgeschlossen werden, dass der Administrator bzw. aufschaltende Mitarbeiter mit besonderen Systemberechtigungen im Rahmen der Aufschaltung Kenntnis personenbezogener Daten erlangt."
>
> BERGBAU, 090201/531/2012

Das Bundesdatenschutzgesetz schreibt für den Umgang mit personenbezogenen Daten den Grundsatz der Datensparsamkeit vor (§ 3a BDSG). Eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist nach § 4 BDSG nur erlaubt, wenn dies durch das BDSG oder eine andere Rechtsvorschrift zugelassen wurde oder die/der Betroffene eingewilligt hat. Auch für das Beschäftigungsverhältnis gilt: Nicht einfach alle anfallenden personenbezogenen Daten dürfen vom Unternehmen genutzt werden. Dies ist grundsätzlich nur im Rahmen des § 32 BDSG zulässig: „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."
Da MDM erfasst auch personenbezogene Daten, die nicht zur Begründung oder für die Durchführung des Beschäftigungsverhältnisses notwendig sind. Daher müssen entweder die Betroffenen zustimmen oder eine Betriebsvereinbarung dient als Rechtsvorschrift im Sinne des § 4 BDSG für die Erhebung, Speicherung und Verarbeitung der Daten (vgl. Kap. 3.4). Die folgende Bestimmung konkretisiert und beschreibt zwar den zulässigen Zweck; sie geht aber über die für das Arbeitsverhältnis erforderlichen Daten hinaus („zur Erreichung des Geschäftszwecks"). Zudem ist der Kreis der Zugriffsberechtigten sehr weit gefasst (alle „berechtigten Nutzer").

> „Personenbezogene Daten werden nur insoweit erhoben, verarbeitet oder genutzt, wie dies zur Erfüllung der Arbeitsaufgabe, zur Erreichung des Geschäftszwecks oder aufgrund gesetzlicher Nachweispflichten erforderlich ist. In der Regel sind dies der Benutzername oder sonstige Identitätskennungen und – soweit erforderlich – die zeitliche Dokumentation von Buchungsvorgängen. Ein Zugriff auf diese Daten ist durch Administratoren und berechtigte Nutzer möglich."
>
> BERGBAU, 090201/531/2012

Die folgende, sehr offene Regelung stützt eine Zweckbindung auf § 31 BDSG (Besondere Zweckbindung). Dieser Paragraph besagt: „Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden." Damit dürfen die Daten ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage verwendet werden. Tatsächlich werden aber Berechtigungen, Beschäftigtendaten, Vorgesetztennamen und Zugangsdaten verwaltet. Dies geht weit über die zulässigen Erhebungen gemäß § 31 BDSG hinaus und stellt somit keine wirksame Rechtsgrundlage dar.

„[Das System] bezieht die Beschäftigtendaten aus der [Bank]-Aufbauorganisation; für jeden Beschäftigten wird der jeweilige Vorgesetzte [im System] hinterlegt. Zur Verwaltung der Berechtigungen ist zudem für jeden Beschäftigten eine sog. […]-ID (= [Bank]-Kennung und [Bank]-Passwort) erforderlich. Nur solche personenbezogenen Daten werden erhoben und verarbeitet, die für das Identity- und Access-Management erforderlich sind. Alle [im System] verarbeiteten personenbezogenen Daten unterliegen der besonderen Zweckbindung des § 31 BDSG."

KREDITGEWERBE, 090202/220/2012

In der folgenden Regelung bleibt unklar, ob eine Leistungskontrolle ermöglicht werden soll oder nicht. Die Zuordnung von Bearbeitungszeiten zu den einzelnen Beschäftigten lässt jedenfalls eine Leistungskontrolle zu. Sollen die Daten beispielsweise nur der Abrechnung gegenüber dem Kunden dienen, wäre es sinnvoll, diese Einschränkung in der Betriebsvereinbarung zu beschreiben.

„Für die Erfassung der Bearbeitungszeit von Aufträgen (Zeitrückmeldung in [Firma]) werden außer dem Namen der AN [Arbeitnehmer] und im Hintergrund der Anwendung die zugehörige Personalnummer keine weiteren personenbezogenen Daten gespeichert."

ENERGIEDIENSTLEISTER, 090202/225/2012

2.6.2 Verpflichtung der Beschäftigten

Die Beschäftigten verfügen auf ihren mobilen Geräten über sehr sensible Unternehmensdaten oder Daten Dritter, die sie anderen offenbaren oder unsachgemäß verwenden könnten. Daher wird ihnen durch Vereinbarungen gern eine Vielzahl von Verpflichtungen auferlegt. Dies mag nötig oder gerechtfertigt sein. Es erfordert aber, dass die Beschäftigten die Verpflichtungen auch umsetzen können. Dafür müssen sie zunächst verstehen, was von ihnen verlangt wird. Angesichts folgender Formulierung stellt sich die Frage: Wie können die Beschäftigten Kenntnis erhalten von den Urheberrechten Dritter oder von Lizenzvereinbarungen, um diese dann zu beachten?

„Für die Einhaltung der Urheberrechte Dritter ist allein der Mitarbeiter verantwortlich. Dies gilt auch für die Beachtung etwaiger Lizenzvereinbarungen."

FAHRZEUGHERSTELLER KRAFTWAGEN, 090202/203/0

Einen besonderen Umgang mit besonders schutzwürdigen Daten von Personen herauszustellen, ist ein sehr guter und wichtiger Ansatz. Aber in der folgenden Vereinbarung ist der Bezug auf § 3 Abs. 9 BDSG als einzuhaltende Vorschrift wenig transparent. Außerdem weist die Einschränkung „insbesondere" darauf hin, dass die Regelung in § 3 Abs. 9 BDSG nicht abschließend sein soll. Gut wäre es, diese kurze Vorschrift zu zitieren: damit sie sofort für die Anwenderinnen und Anwender nachlesbar ist und um klarzustellen, um welche Daten es sich darüber hinaus handelt: „§ 3 Abs. 9 BDSG – Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben." Leider wird der Inhalt des Wortes „grundsätzlich" in juristischen Zusammenhängen häufig verkannt. Es beinhaltet gerade *keinen* vollständigen Ausschluss, sondern lässt Ausnahmen zu. Mit der nachstehenden Regelung wird nur grundsätzlich die Verarbeitung von besonders schutzwürdigen personenbezogenen Daten ausgeschlossen – daher bleibt offen, wann eine Verarbeitung zulässig ist.

„Die Verarbeitung besonders schutzwürdiger personenbezogener Daten am häuslichen Arbeitsplatz und unterwegs ist grundsätzlich untersagt. Hierzu zählt insbesondere die Verarbeitung der in § 3 Absatz 9 Bundesdatenschutzgesetz aufgeführten sensiblen Daten."

ÖFFENTLICHE VERWALTUNG, 080102/223/2013

Folgende Vereinbarung lässt die genauen Sicherheitsvorschriften, die die Beschäftigten zu beachten haben, offen und verweist auf die Sicherheitsrichtlinien im Intranet. Das hat den Vorteil, dass diese Richtlinien den jeweiligen Erfordernissen neuer Geräte oder veränderter Technik angepasst werden können. Um Änderungen für die Betroffenen erkennbar zu machen, sollen diese ausdrücklich bekannt gegeben werden.

„Die berechtigten Beschäftigten sind gehalten, sich vorab und auch in regelmäßigen Abständen bezüglich des Anmeldeverfahrens mittels Token [...] und der aktuellen Sicherheitsrichtlinie zur Nutzung von mobilen Arbeitsmöglichkeiten über Fernzugriff [in der Firma] zu informieren. Die jeweils gültigen Informationen sind im Intranet [der Firma] (IT-Portal) eingestellt. Änderungen des Anmeldeverfahrens und der Sicherheitsrichtlinie werden den Token-Nutzern im Intranet bekannt gegeben."

ÖFFENTLICHE VERWALTUNG, 080102/223/2013

Die folgende Erklärung versucht, die persönliche Einwilligung mit abzubilden, die gemäß § 4 BDSG zur Datenverarbeitung gegebenenfalls erforderlich ist. Sie erfüllt aber nicht die Anforderungen des § 4a Abs. 1 BDSG, da der Zweck der Verarbeitung nicht erkennbar wird. Im Gesetzestext heißt es: „§ 4a BDSG – Einwilligung (1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben."
Gleichzeitig werden die Beschäftigten in die Pflicht genommen, die Nutzungsbestimmungen für die mobilen Geräte zu beachten. Idealerweise sind die Nutzungsbestimmungen nachlesbar und die zu verarbeitenden personenbezogenen Daten in einem Anhang zur Betriebsvereinbarung konkretisiert und damit erkennbar.

„Ich verpflichte mich zur Einhaltung der Nutzungsbestimmungen für das mobile Endgerät und erkläre mich damit einverstanden, dass mein mobiles Endgerät über die Mobile Device Management-Software [Firma] administriert und bei Verlust administrativ gelöscht werden wird. Eine Abschrift dieser Nutzungsbestimmungen habe ich erhalten. Ich erkläre mich weiterhin damit einverstanden, dass meine personenbezogenen Daten im Mobile Device Management System [Firma] verarbeitet werden."

VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Eingriffe in Rechte der Beschäftigten werden insbesondere durch ein Speicherverbot von privaten Daten auf den Geräten verhindert. Dieses Verbot gilt jedoch nur „grundsätzlich". Daher stellt sich die Frage nach den zulässigen Ausnahmen – die jedoch nicht beantwortet wird.

„Auf mobilen Endgeräten dürfen grundsätzlich keine privaten Daten gespeichert werden."

ÖFFENTLICHE VERWALTUNG, 090202/137/2009

2.6.3 Verpflichtung von Familienangehörigen

MDM kann den Zugriff auf Firmendaten über mobile Geräte zulassen. Daher haben die Unternehmen ein großes Interesse daran, diesen Zugriff nur Berechtigten zu ermöglichen. Laut folgender Regelung müssen die Beschäftigten bei mobiler Arbeit den Zugriff und die Einsichtnahme durch Dritte verhindern. Dies gilt auch für Familienangehörige.

> „Die Beschäftigten verpflichten sich, Daten und Informationen im Rahmen der Telearbeit und der Mobilen Arbeit so zu schützen, dass Dritte weder Einsicht noch Zugriff nehmen können. Die ‚Sicherheitsrichtlinie zur Nutzung von mobilen Arbeitsmöglichkeiten über Fernzugriff im [Firma]' in der jeweils gültigen Fassung ist zu beachten."
>
> ÖFFENTLICHE VERWALTUNG, 080102/223/2013

Das gewünschte Ziel, auch die Haushaltsangehörigen zu verpflichten, wird mit der nachstehenden Bestimmung nicht erreicht. Vereinbarungen zulasten Dritter sind nicht wirksam, wenn die Dritten nicht ausdrücklich zustimmen. In einer Betriebsvereinbarung können Regeln für die Beschäftigten des Unternehmens aufgestellt werden, aber nicht für außenstehende Dritte. Auch eine „Sippenhaft" ist dem deutschen Rechtssystem fremd.

> „Im Falle der Beschädigung von [Firmen]-eigenen Arbeitsmitteln – einschließlich deren Verlustes bzw. des Verlustes von Datenbeständen – haften die Beschäftigten (einschließlich Haushaltsangehörige oder berechtigt in der Wohnung befindliche Dritte) nur, wenn die Beschädigung bzw. der Datenverlust vorsätzlich oder grob fahrlässig verursacht wurde."
>
> ÖFFENTLICHE VERWALTUNG, 080102/223/2013

Die Problematik der unwirksamen Regelungen zulasten Dritter umgeht die folgende Vereinbarung, indem sie den Haushaltsangehörigen eine Verpflichtungserklärung abverlangt. Eine solche Verpflichtung kann nicht erzwungen werden. Wird sie jedoch nicht abgegeben oder später widerrufen, endet die Erlaubnis zu mobiler Arbeit gemäß der Vereinbarung durch die Betriebsparteien.

> „Die Beschäftigten und die in häuslicher Gemeinschaft lebenden Familienangehörigen erklären sich [...] bei mobiler Arbeit damit einverstanden, für Kontrollzwecke der/dem Datenschutzbeauftragten der Dienststelle und dem Bundesbeauftragten für den Datenschutz sowie Vertretern der für Datenschutz und IT-Sicherheit zuständigen Organisationseinheiten Zugang zum häuslichen Arbeitsbereich zu gewähren. Ein Widerruf der Einverständniserklärung führt zu der sofortigen Beendigung."
>
> VERWALTUNG, 080102/223/2013

2.6.4 Zugriffsrechte des Unternehmens

Eine wichtige Funktion von MDM ist die mögliche Löschung von Daten auf dem mobilen Gerät per Fernzugriff. Im Fall eines Verlustes des Gerätes ist dies eine wichtige Möglichkeit, die Firmendaten vor dem Zugriff unbefugter Dritter zu schützen. Die nachfolgende Regelung stellt es den Betroffenen frei, ob auch ihre privaten Daten gelöscht werden sollen.

„Die Arbeitnehmer werden darauf hingewiesen, dass mittels [Firma] die technische Möglichkeit besteht – insbesondere im Falle des Verlusts des iPads – sämtliche auf dem iPad vorhandenen Daten, Anwendungen usw. per Fernzugriff zu löschen. Dem Mitarbeiter wird daher angeraten, selbst für eine ausreichende Backup-Sicherung für seine private Daten, Anwendungen usw. Sorge zu tragen. Der Mitarbeiter kann entscheiden, ob im Falle eines Verlustes des iPads neben den dienstlichen Funktionen auch private Daten, Anwendungen etc. gelöscht werden sollen."

CHEMISCHE INDUSTRIE, 050340/39/2012

Einen Schritt weiter geht die folgende Vereinbarung: Der bzw. die betroffene Beschäftigte muss kontaktiert werden, bevor eine Löschung aktiviert wird.

„Stellt die [Firma] einen unberechtigten Zugriff Dritter auf ein mobiles Endgerät fest, wird ein Schadprogramm auf einem mobilen Endgerät verwendet oder droht das Firmennetzwerk durch andere Zugriffe beschädigt zu werden, hat sie unverzüglich Kontakt zu den betroffenen Beschäftigten Kontakt aufzunehmen und sie darüber zu informieren. Bevor ein Remote-Löschprozess in Gang gesetzt wird, muss den Beschäftigten die Möglichkeit eingeräumt werden, ihre privaten Daten zu sichern."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Einen größeren Schutz des Unternehmens verfolgt der folgende Automatismus. Die Wahrscheinlichkeit einer unbefugten Nutzung ist sehr groß, wenn jemand das Passwort zu dem Gerät nicht kennt. Daher werden bei 10-facher Fehleingabe alle Daten auf dem Gerät gelöscht – auch die privaten. Sie sind damit zwar verloren, aber auch vor dem Zugriff Unbefugter geschützt.

„Außerdem ist festgelegt, dass nach 10 ungültigen Codeeingaben sämtliche Daten auf dem Gerät gelöscht werden. Diese Einstellungen werden durch das MDM Provisioning-Zertifikat der betreffenden IT-Abteilung verwaltet."

CHEMISCHE INDUSTRIE, 090202/190/2012

2.6.5 Speicherung – Umfang, Ort, Dauer

Das Bundesverfassungsgericht hat in den vergangenen Jahren den Schutz der Persönlichkeit herausgestellt. Es betonte im Jahr 2008, dass das allgemeine Persönlichkeitsrecht in Art. 2 Abs. 1 und Art. 1 Abs. 1 GG das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst (BVerfG vom 27.2.2008 – 1 BvR 370/07). Grundgedanke ist der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten sowie die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfG vom 15.12.1983 – 1 BvR 209/83). Daher ist richtigerweise laut folgender Vereinbarung eine Weitergabe von personenbezogenen Daten an Dritte untersagt.

„Eine Weitergabe personenbezogener oder privater Daten der Beschäftigten ist der [Firma] untersagt. Hinsichtlich der personenbezogenen Daten hat die [Firma] die Vorgaben des BDSG zu beachten."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Eine andere Frage betrifft die Dauer der Speicherung. Der Grundsatz der Datensparsamkeit des § 3a BDSG bedeutet auch: Eine Speicherung erfolgt nur so lange, wie es für den Erhebungszweck nötig ist. Für die Beschäftigten wäre es notwendig, konkret nachlesen zu können,

wie lang welche Daten gespeichert werden. Diesem Anspruch wird die folgende Regelung nicht gerecht.

> „Personenbezogene Daten der Beschäftigten in oder in Verknüpfung mit Nutzungs- und Verbindungsdaten sind nur so lange zu speichern, wie dies notwendig oder gesetzlich vorgeschrieben ist."
>
> ÖFFENTLICHE VERWALTUNG, 090202/137/2009

Die nachstehende Vereinbarung erfüllt den Anspruch, möglichst keine unnötige Speicherung vorzunehmen. Allerdings stellen sich die Fragen: Welcher Zweck ist gemeint? Über welche Zeitspanne ist eine Speicherung danach nötig und möglich?

> „Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Mitarbeiter entgegenstehen, es sei denn, die Daten sind Gegenstand eines konkreten Ermittlungsverfahrens."
>
> GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Im folgenden Ansatz wurde genau überlegt, welche Daten wie lang gebraucht werden; eine „lebenslange" Speicherung gilt als erforderlich. Für die Zeit der Nutzung durch die bzw. den Beschäftigten ist das nachvollziehbar, wird jedoch in der Klausel nicht deutlich.

> „Eine Löschung der Konfigurationsdaten der Geräte (beinhaltet zusätzlich nur den Nutzernamen des Mitarbeiters) ist derzeit im System nicht vorgesehen, da dies eine Voraussetzung zur lebenslangen Dokumentation (Eindeutigkeit) bzw. Wiederfindung (Verlust, Diebstahl) ist."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Gut kontrollierbar und administrierbar ist die folgende klare und einfache Regel. Wahrscheinlich sind die 14 Monate ein Kompromiss der Betriebsparteien bei der Verhandlung der Betriebsvereinbarung. Denn ein Bezug zu gesetzlichen Fristen oder dergleichen wird nicht hergestellt.

> „Auswertungen mit personenbezogenen oder personenbeziehbaren Daten sind nach 14 Monaten zu vernichten."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

2.6.6 Private Daten

Sobald die private Nutzung von mobilen Geräten erlaubt ist, entstehen unterschiedliche Regelungsbedürfnisse. Die Beschäftigten haben einen Anspruch darauf, ihre Daten vor dem Zugriff über MDM durch den Arbeitgeber zu schützen. Dieses Ziel wird mit dem klaren Verbot in folgender Regelung erreicht.

> „Die [Firma] stellt sicher, dass personenbezogene, private und geschäftliche Daten getrennt voneinander, beispielsweise durch getrennte Mail-Konten auf dem mobilen Endgerät verwaltet werden. Ein Zugriff auf private Daten ist der [Firma] nicht gestattet."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Im Idealfall ist der Zugriff auf die privaten Daten genauso geschützt, wie der Zugriff auf die Unternehmensdaten. Dies verfolgten die Betriebsparteien im Folgenden und konnten es umsetzen.

> „Die [Firma] stellt weiter sicher, dass sämtliche personenbezogenen und privaten Daten der Beschäftigte/innen gegen Zugriffe Dritter und externer Stellen geschützt werden. Sie hat hierüber einen Nachweis zu erbringen, welche Sicherheitsvorkehrungen getroffen werden."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Zusätzlich wird den Beschäftigten ein Auskunftsanspruch eingeräumt. Dieser beinhaltet auch den Nachweis, dass keine Dritten auf die privaten Daten zugegriffen haben. In der Praxis könnte es sehr schwierig werden, etwas nachzuweisen, das nicht passiert ist.

> „Er/sie kann verlangen, dass die [Firma] nachweist, dass Sicherheitsvorkehrungen zum Schutz seiner/ihrer Daten getroffen wurden und ein Zugriff durch Dritte nicht erfolgt ist."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Häufig stellt MDM durch Backups sicher, dass die Daten mobiler Geräte reproduzierbar sind. Werden Geräte von unterschiedlichen Beschäftigten nacheinander genutzt oder getauscht, muss sichergestellt sein, dass die privaten Daten nicht per Backup wieder aufgespielt werden. Der Anspruch auf eine derartige Löschung ist in § 35 BDSG verbrieft. Er müsste nicht in einer Betriebsvereinbarung wiederholt werden. Einfacher wäre es, wenn den Unternehmen auch ohne Antrag der Betroffenen die Pflicht zum Löschen auferlegt würde.

> „Die Nutzer von mobilen Endgeräten haben das Recht, Auskunft über ihre gespeicherten Daten zu verlangen (§ 34 BDSG). Beim Vorliegen sachlicher Voraussetzungen (z. B. bei Rückgabe des mobilen Endgerätes) können sie zudem die Löschung oder Änderung ihrer gespeicherten Daten verlangen (§ 35 BDSG)."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

2.7 Leistungs- und Verhaltenskontrolle

Durch das mögliche Erfassen einer Vielzahl von Nutzungsdaten wird das Arbeitsverhalten der Beschäftigten transparent und nachvollziehbar. Die Daten können gespeichert und ausgewertet werden. Leistungs- und Verhaltenskontrollen unterliegend der Mitbestimmung des Betriebsrates (§ 87 Abs. 1 Nr. 6 BetrVG). Daher ist die Regelung dieses Bereiches ein wichtiger Aspekt in den Vereinbarungen. Die folgende Regelung wirft jedoch die Frage auf: Erfolgte eine Zustimmung durch die Hintertür? Oder wurde bewusst auf Mitbestimmungsrechte verzichtet? Diese Regelung allein wäre zu wenig. Sie steht so in der Vereinbarung, da vorher die zulässigen Auswertungen genau benannt wurden.

> „Informationen über die durchgeführten Maßnahmen werden dem Betriebsrat jederzeit zur Verfügung gestellt."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Eine andere Idee besteht darin, den Betriebsrat in den Auswertungsprozess einzubeziehen. Damit übernimmt er zugleich eine große Verantwortung. Unklar bleibt bei folgender Formulierung: Wird die Frage der Zulässigkeit von Auswertungen durch Mehrheitsentscheid ent-

schieden? Oder hat das Betriebsratsmitglied bzw. die/der Datenschutzbeauftragte ein Vetorecht?

> „Die personenbezogene Auswertung erfolgt durch ein Gremium, bestehend aus dem jeweiligen Systemadministrator oder dessen Stellvertreter, dem Betriebsratsvorsitzenden oder dessen Stellvertreter sowie dem Datenschutzbeauftragten."
>
> GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Zu bevorzugen sind klare eindeutige Regeln und Öffnungsmöglichkeiten nur, wenn der Betriebsrat als Gremium dem zugestimmt hat.

2.7.1 Ausschluss von Auswertungen

Optimal sind die Beschäftigten geschützt, wenn Auswertungen völlig ausgeschlossen werden. Insbesondere der zweite Satz in nachfolgendem Beispiel regelt diesen Ausschluss einfach und klar.

> „Arbeitgeber und Betriebsrat sind sich darüber einig, dass die eingesetzte Telekommunikationsdaten und -systeme nicht für den Zweck der Leistungs- und Verhaltenskontrolle der Mitarbeiter eingesetzt werden. Es findet keine Leistungs- oder Verhaltenskontrolle von Mitarbeitern statt."
>
> GESUNDHEIT UND SOZIALES, 090202/201/2013

Kein vollständiger Ausschluss wird mit der nachstehenden Bestimmung erreicht. Denn Auswertungen gemäß Ziffer 2 der Vereinbarung sind ausgenommen. Ziffer 2 formuliert die Auswertungsmöglichkeit des „Verkehrsvolumens" – der Anzahl der aus- und eingehenden E-Mails. Diese Zahl kann eine quantitative Leistungskontrolle ermöglichen.

> „Eine Überwachung von Leistung oder Verhalten im Sinne des § 87 Abs. 1 Ziffer 6 BetrVG findet über den nach Ziffer 2 vordefinierten Zweck nicht statt, d. h. darüber hinausgehende diesbezügliche personenbezogene Auswertungen werden nicht durchgeführt."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Nach der folgenden Klausel dürfen die protokollierten Daten nicht für personenbezogene Nutzerprofile verwendet werden. Das klingt, als wären andere Auswertungen und eine Nutzung zur Steuerung (aus den aktuell einsehbaren Daten) möglich und zulässig. Eindeutiger sind Negativ- oder Positivlisten mit den zulässigen oder untersagten Auswertungsmöglichkeiten.

> „Eine Protokollierung und Überwachung der Kommunikation der einzelnen Beschäftigten und die Erstellung von personenbezogenen Nutzerprofilen anhand der von [der Firma] protokollierten Daten findet nicht statt und ist ausdrücklich untersagt."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Allerdings ist die folgende Negativliste sehr kurz. Sie ermöglicht im Umkehrschluss – erlaubt ist alles, was nicht verboten ist – doch eine Vielzahl von Auswertungen.

> „Datenerhebung zu Kundenbesuchen und Kundengesprächen werden ausgeschlossen. Die Verteilung der Apps erfolgt über das MDM Tool."
>
> PAPIERGEWERBE, 090202/202/2013

Klar und umfassend ist der Ausschluss aller Daten, die entstehen können und verarbeitet werden, in folgender Bestimmung.

> „Alle Daten auf mobilen Endgeräten und Verbindungsdaten, die bei der Nutzung der Geräte entstehen, dürfen nicht zur Leistungs- und Verhaltenskontrolle ausgewertet werden. Ortungen oder das Erstellen von Bewegungsprofilen sind unzulässig."
>
> ÖFFENTLICHE VERWALTUNG, 090202/137/2009

2.7.2 Auswertungen ohne Kontrollfunktion

Die Verwaltung der Geräte und der Software auf den Geräten durch MDM dient auch dazu, ihre technische Sicherheit zu gewährleisten und ihre Funktionsfähigkeit zu erhalten. Die hiermit verbundenen Auswertungen beschäftigen sich mit unterschiedlichen Aspekten: Wie aktuell sind die Daten seit dem letzten Update? Wie lässt sich Schadsoftware auf den Geräten verhindern? Wie lässt sich vermeiden, dass Schadsoftware ins Unternehmen eingeschleust wird? Diese Zielrichtung spiegelt die folgende Regelung wieder. Noch vorteilhafter wäre es gewesen, wenn die Verkehrsdaten – der Zugriff auf E-Mail-Dienste, Verkehrsvolumen etc. – anonymisiert erhoben werden müssten.

> „Die Auswertung der Daten erfolgt über eine zugriffsgeschützte Web-Anwendung. Es werden folgende Auswertungen durchgeführt:
> - Status der Softwareverteilung/Updates
> - Compliance des Endgerätes (z. B. Jailbreaks, nicht aktuelle Patches, verbotene Software)
> - Status des Endgerätes (z. B. letzte Verbindung zum Lizenzmanagement, Zugriff des Endgerätes auf E-Maildienste)
> - Verkehrsvolumen (z. B. Zahl ein- und ausgehender Mails).
>
> Die für die Auswertungen erforderlichen Datenfelder sind in Anlage 2 abschließend aufgeführt."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

In der nachfolgenden Regelung geht es um technische Fragen und Gebührenabrechnungen. Auch diese Daten könnten größtenteils anonymisiert oder gruppenbasiert ausgewertet werden.

> „Im Auftrag der Bank erstellt der Dienstleister
> - Auswertungen, die als Nachweis zur Erfüllung der vereinbarten Service Level Agreements (SLA) notwendig sind. Diese Auswertungen betreffen die Qualität, Verfügbarkeit, Performanz und Auslastung der Systemkomponenten,
> - Verbindungsstatistiken pro Kostenstelle,
> - Gebührenabrechnungen gem. A §§ 6 und 10 Abs. 2."
>
> KREDITGEWERBE, 090202/220/2012

Nachstehend ist die Erfassung von Einzelverbindungsdaten untersagt. Ideal ist die hier gefundene Lösung, die Funktion im System zu deaktivieren. So ist eine missbräuchliche Auswertung von vornherein ausgeschlossen.

„Das MDM erlaubt grundsätzlich den Zugriff auf die im Zusammenhang mit der Nutzung erfassten technischen und personenbezogenen Daten. Bei der Nutzung werden technische Statusdaten (z. B. Speicherplatzvolumen, Version der Anwendungen), Daten des Gerätes (z. B. Endgeräte-ID), Verbindungsdaten (z. B. genutztes Telekommunikationsnetzwerk) und Nutzungsdaten (z. B. Datenvolumen) durch das MDM verarbeitet. Sofern das System die Erfassung von Einzelverbindungsdaten ermöglicht, ist diese Funktion durch den Systembetreiber zu deaktivieren."

BERGBAU, 090201/531/2012

Im Gegensatz dazu wird laut nachfolgender Bestimmung eine Menge an Daten erfasst und deren Nutzung durch die Vereinbarung begrenzt. Es bleibt offen, wie der Betriebsrat die Einhaltung dieser Regelung kontrollieren kann.

„Protokolldaten über die Inventardaten, die Nutzung der mobilen Endgeräte sowie die Nutzung der von der Mediengruppe [Firma] bereitgestellten Services (z. B. E-Mail-/Exchange) werden – sofern sie Mitarbeiterkennzeichen enthalten – nur verwendet, um bei Nachfragen im Zusammenhang mit einem einzelnen Vorgang eine verantwortliche Person kenntlich zu machen. Sie dürfen nur zum Zweck der Datenschutzkontrolle, der Datensicherung, der Sicherstellung des ordnungsgemäßen Betriebs der mobilen Endgeräte, der Fehleranalyse oder -korrektur und der Systemoptimierung einschließlich Kapazitätsplanung gespeichert und verwendet werden."

VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

2.7.3 Anlassbezogene Auswertungen

Die missbräuchliche oder strafrechtlich relevante Nutzung von mobilen Geräten kann über MDM-Systeme aufgedeckt werden. In der Betriebsvereinbarung wird die „Eingriffsschwelle" festgelegt: Unter welchen Umständen darf was ausgewertet werden? Laut folgendem Textauszug genügen schon „Unregelmäßigkeiten oder ein begründeter Verdacht auf Unregelmäßigkeiten bei der Nutzung" für eine personenbezogene Auswertung, wenn der Betriebsrat zustimmt. Was wird jedoch unter Unregelmäßigkeiten verstanden? Diese Frage bleibt offen.

„Sollten Unregelmäßigkeiten oder ein begründeter Verdacht auf Unregelmäßigkeiten bei der Nutzung einzelner Geräte oder durch einzelne Mitarbeiter eine punktuelle oder zeitnahe Prüfung erfordern, dürfen die Daten mit Zustimmung des Betriebsrats technisch gesichert werden und Einzelverbindungsnachweise unter Einbindung des Betriebsrats ausgewertet werden."

GESUNDHEIT UND SOZIALES, 090202/201/2013

In der nächsten Bestimmung wird eine missbräuchliche Nutzung neben eine Straftat gestellt. Auch hier wäre es vorteilhaft für die Beschäftigten, wenn klargestellt würde, was unter missbräuchlicher Nutzung beispielsweise verstanden wird.

„Unter den Voraussetzungen des § 7 ist daneben eine Verwendung der erfassten Daten zur Aufklärung einer missbräuchlichen Nutzung und der Begehung von Straftaten zulässig."

GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Die folgende Vereinbarung schließt eine Leistungs- und Verhaltenskontrolle mittels erhobener Daten aus. Ausnahmen gibt es nur, wenn Beschäftigte gegen die Betriebsvereinbarung oder

gegen behördliche bzw. gesetzliche Verpflichtungen verstoßen. Sollte der Arbeitgeber diesen Rahmen selbst missbrauchen, darf er darauf keine arbeitsrechtlichen Sanktionen stützen.

> „Durch die iPads und anhand der mittels dieser erhobenen Daten erfolgt keine Leistungs- oder Verhaltenskontrolle. Dies gilt nicht für die Feststellung von Verstößen von Mitarbeitern gegen ihre Verpflichtungen aus Betriebsvereinbarungen und Verpflichtungen aus behördlichen bzw. gesetzlichen Auflagen (z. B. Dokumentationspflicht gemäß HWG). Soweit Daten unter Verstoß gegen diese Betriebsvereinbarung gewonnen werden, dürfen darauf keine personellen Einzelmaßnahmen gestützt werden."
>
> CHEMISCHE INDUSTRIE, 050340/39/2012

2.7.4 Überwachung – Ort

MDM kann durch GPS jederzeit feststellen, wo sich ein mobiles Gerät derzeit befindet. Werden diese Daten gespeichert, lassen sich damit Bewegungsprofile der Nutzerinnen und Nutzer erstellen. Auswertungen zeigen ferner: Wer war wo und wie lang? Dadurch wird insgesamt eine sehr umfassende, tief in Persönlichkeitsrechte eingreifende Leistungs- und Verhaltenskontrolle möglich. Dies wird mit der folgenden Regelung ausgeschlossen. Zudem können die Beschäftigten den Ortungsdienst abschalten.

> „Über den sogenannten Ortungsdienst (Lokalisationservice) des Endgeräterstellers kann der Status des Gerätes (Jailbreak Ja/Nein) überprüft werden. Dafür werden Daten des Ortungsdienstes genutzt. Diese Daten werden ausschließlich für die Sicherstellung der Compliance verwendet. Es können keine Bewegungsprofile der Benutzer erstellt werden. Es erfolgt keine Speicherung historischer Daten am Server. Die Erfassung der Ortungsdaten kann vom Benutzer abgeschaltet werden. Dies bedingt dann aber automatisch die Trennung vom [Firmen]-Netz. Wird der Ortungsdienst wieder aktiviert, muss der Mitarbeiter die E-Mail-Synchronisation über den IT-Shop aktivieren."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Im Gegensatz zu der Nutzung von GPS-Daten und ihrer Speicherung steht das Abschalten. Gemäß folgender Vereinbarung werden diese Daten nicht erhoben. Damit muss die Zulässigkeit der Auswertung nicht mehr kontrolliert werden.

> „Die GPS-Funktionalität der [Firma] wird ebenfalls durch die ZDV [Zentrale Datenverarbeitung] dauerhaft außer Betrieb gesetzt, so dass eine Ortung oder Wegverfolgung über die Endgeräte nicht möglich ist."
>
> GESUNDHEIT UND SOZIALES, 090202/201/2013

Begründet wird die Sinnhaftigkeit und Notwendigkeit des Ortungsdienstes damit, das Gerät im Diebstahlsfall wieder auffinden zu können. Bisher liegen jedoch keine Erkenntnisse vor, dass in der Praxis dadurch tatsächlich Geräte gefunden wurden. Der technisch versierte Dieb wird vermutlich zuerst die GPS-Funktion deaktivieren. Für das durchaus sinnvolle Löschen der Unternehmensdaten auf den mobilen Geräten per Fernzugriff muss keine Ortung erfolgen. Es genügt, das Gerät per Remote erreichen zu können. Folgerichtig werden in der nachstehenden Vereinbarung jegliche Protokollierung, Speicherung und Überwachung der Geräte per GPS und MDM ausgeschlossen, indem sie deaktiviert werden.

„Eine Protokollierung, Speicherung und Überwachung der GPS-Mobilitätsdaten der einzelnen mobilen Endgeräte der Beschäftigten durch [Firma] ist nicht aktiviert und findet nicht statt."

VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Im Folgenden vereinbarten die Betriebsparteien zwar keine Deaktivierung; der zulässige Zugriff ist jedoch ausgeschlossen, soweit nicht ein Diebstahl oder sonstiger Verlust vorliegt. Auch dies stellt eine gute Möglichkeit dar, die Beschäftigten zu schützen. Allerdings bleibt erneut eine Frage offen: Wie kann dieser Ausschluss kontrolliert werden?

„Die [Firma] ist weder innerhalb der individuellen Arbeitszeit noch darüber hinaus dazu berechtigt, eine Lokalisierung des/der jeweiligen Beschäftigten vorzunehmen. Zulässig ist die Lokalisierung des mobilen Endgerätes im Falle des Verlustes und der zuvor angezeigten Verlustmeldung durch die Beschäftigten."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

2.7.5 Überwachung – Zeit

Die Abrechnung der Arbeitszeit für bestimmte Auftraggeber kann über MDM erfolgen. Damit wird beispielsweise erkennbar, wie lange die Technikerin vor Ort war, um eine Reparatur auszuführen. Dies wird in der nachstehenden Vereinbarung entsprechend geregelt. Dabei handelt es sich um personenbezogene Daten. Daher ist eine Regelung nötig, um eine sonstige Nutzung auszuschließen.

„Die Erfassung der Bearbeitungszeit von Aufträgen (Zeitrückmeldung in [Firma]) erfolgt unter Zuhilfenahme der mobilen Endgeräte von den AN [Arbeitnehmern] vor Ort. Sind mehrere AN gemeinsam im Einsatz, werden die Eingaben von einem AN erfasst. Der Erfasser wird dabei dokumentiert."

ENERGIEDIENSTLEISTER, 090202/225/2012

Sehr viele Türen für Leistungs- und Verhaltenskontrollen öffnet die nachstehende Bestimmung. Es genügt ein mit Tatsachen begründeter Verdacht, dass gegen Arbeitsanweisungen verstoßen wurde, um Auswertungen zu ermöglichen. Aber: Der Betriebsrat muss ausdrücklich zustimmen. Damit hat er es in der Hand, ob die Tür geöffnet wird oder nicht. Eine Ausnahme bleibt: Kommt es zu einer außerordentlichen Kündigung, kann ohne Zustimmung des Betriebsrates ausgewertet werden. Das setzt einen entsprechend schwerwiegenden Verstoß der bzw. des Betroffenen voraus.

„Obzwar dazu geeignet, ist Leistungs- oder Verhaltenskontrolle nicht das Ziel der Bank bei der Einführung und Anwendung [des Systems]. Die Bank verpflichtet sich deshalb, Daten [des Systems] nicht zur Grundlage arbeitsrechtlicher Maßnahmen (Sanktionen) zu machen, es sei denn, es besteht der mit Tatsachen begründete Verdacht, dass gegen ausdrückliche Arbeitsanweisungen, Gesetze oder wesentliche arbeitsvertragliche Pflichten verstoßen wurde. In diesem Fall dürfen die hierzu erforderlichen Daten erhoben und genutzt werden, wenn der zuständige Betriebsrat (BR) zuvor schriftlich informiert wurde und zugestimmt hat. Einer Zustimmung bedarf es nicht im Fall der außerordentlichen Kündigung. In betriebsratslosen organisatorischen Einheiten ist der GBR zuvor schriftlich zu informieren."

KREDITGEWERBE, 090202/220/2012

Eine einfache Regelung, um Bewegungsprofile der Beschäftigten zu verhindern, fanden die Parteien im Folgenden: Sie verteilen die Geräte einfach anonym. Damit kann zwar ein Bewegungsprofil des Gerätes aufgezeichnet, aber eben nicht einer bzw. einem bestimmten Beschäftigten zugeordnet werden. Private Daten können die Beschäftigten auf diesen Geräten dann sinnvollerweise nicht mehr speichern, da die Geräte ständig ihren Besitzer wechseln.

> „Diese ‚Bewegungsdaten' werden durch zufällige Vergabe der Geräte zu Beginn der Schicht ohne Protokollierung anonymisiert. Diese willkürliche Verteilung der Mobilgeräte wird täglich durch den Koordinator handschriftlich dokumentiert. Die Dokumentation verbleibt am Arbeitsplatz des Koordinators."
>
> GESUNDHEIT UND SOZIALES, 090202/201/2013

2.7.6 Direkte Kontrollmöglichkeiten

MDM kann mobile Geräte beobachten, indem es sich auf sie „aufschaltet". Es wird erkennbar, welche Anwendung gerade benutzt wird, welche Daten eingegeben werden und so weiter. Hat das mobile Gerät eine Kamera, kann diese über MDM aktiviert werden und somit das Geschehen direkt beobachtet, gefilmt und ferngespeichert werden. Das Bundesarbeitsgericht entschied bereits 1987, dass eine lückenlose Aufzeichnung der Tätigkeiten der Beschäftigten durch Kameras unzulässig in ihre Persönlichkeitsrechte eingreift (BAG vom 7.10.1987, Az.: 5 AZR 116/86). Dabei reicht es aus, dass die Beschäftigten befürchten müssen, während der Arbeit mit Hilfe technischer oder elektronischer Kontrolleinrichtungen jederzeit beobachtet oder in anderer Weise fortlaufend kontrolliert zu werden. Dieser entstehende Überwachungsdruck behindert die Beschäftigten in der freien Entfaltung ihrer Persönlichkeit (BVerwG vom 23.09.1992, Az.: 6 P 26/90; BAG vom 14.09.1984, Az.: 1 ABR 23/82).
Das LAG Hamm geht einen Schritt weiter: Ihm zufolge könnten auch zeitlich limitierte Filmaufnahmen das Persönlichkeitsrecht der Beschäftigten verletzen (LAG Hamm vom 30.12.2012, Az.: 9 Sa 158/12): „Soweit der Arbeitnehmer nicht weiß, wann eine Überwachungskamera an seinem Arbeitsplatz in Betrieb ist und er den genauen Erfassungsbereich nicht kennt, ist er in einem über die rein objektive Beobachtungszeit hinausgehenden Zeitraum dem Anpassungsdruck ausgesetzt, auch wenn dieser keineswegs während der jeweiligen vollen Arbeitsschicht vorliegt."
Die nachfolgende Regelung schließt das Aufschalten während einer „Benutzersitzung" aus, wenn die Beschäftigten nicht zustimmen. Mit Benutzersitzung ist wahrscheinlich die aktive Nutzung des mobilen Gerätes durch die bzw. den Beschäftigten gemeint. Es stellt sich die Frage: Wie kann kontrolliert werden, dass diese Regelung eingehalten wird?

> „Zur Erreichung des genannten Zwecks kann sich ein Administrator bzw. Mitarbeiter mit besonderen Systemberechtigungen jederzeit – ggf. auch bei ausgeschaltetem Endgerät und ohne Mitwirkung des Anwenders – per Fernwartungssoftware auf das Endgerät schalten. In einer laufenden Benutzersitzung erfolgt die Aufschaltung jedoch nur nach Zustimmung des Anwenders. Eine darüber hinausgehende Aufzeichnung der Aufschaltungssitzung wird nur in Ausnahmefällen nach vorhergehender Vereinbarung zwischen Aufschaltendem und Anwender durchgeführt."
>
> BERGBAU, 090201/531/2012

Ein erweitertes Verbot des Online-Zugriffs wird im Folgenden formuliert: Die Persönlichkeitsrechte der Beschäftigten werden über die Interessen der Dienststelle gestellt. Zugriffe erfordern danach die Kenntnis und Zustimmung der Betroffenen. Über Protokolldaten im MDM-System sollten unzulässige Zugriffe erkennbar werden.

„Zugriffe auf ein mobiles Endgerät über Online-Verbindungen ohne Kenntnis und Zustimmung des/der Beschäftigten, dem/der das Endgerät dienstlich überlassen wurde, sind unzulässig."

ÖFFENTLICHE VERWALTUNG, 090202/137/2009

Indem der Echtzeit-Remote-Zugriff technisch ausgeschlossen ist, sind die Beschäftigten nachstehend vor ständiger Überwachung und der Verletzung ihrer Persönlichkeitsrechte geschützt. Die Kontrolle ist einfach, da nur der technische Ausschluss überprüft werden muss.

„Die [Firma] führt über das MDM-System eine regelmäßige Datenprüfung der auf den mobilen Endgeräten gespeicherten Daten während der individuellen Arbeitszeit der Beschäftigten durch. Dabei wird lediglich eine Kontrolle durchgeführt, ob unberechtigte Zugriffe durch Dritte erfolgen oder sich Schadprogramme/Viren auf dem mobilen Endgerät befinden. Ein Echtzeit-Remote-Zugriff wird technisch ausgeschlossen."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

2.8 Gesundheitsschutz

Die Möglichkeit, mit mobilen Geräten zu jeder Zeit an jedem Ort arbeiten zu können, wird bereits in vielen Betriebsvereinbarungen durch begrenzende Vorschriften eingeschränkt: E-Mails werden nach bestimmten Zeiten nicht mehr zugestellt; die Zugänge zu den Unternehmenssystemen zu bestimmten Zeiten gesperrt. Aber auch das System, die Software an sich, kann gesundheitliche Beeinträchtigungen auslösen. Verschiedene Faktoren können sich negativ auf die Gesundheit auswirken: das Wissen um die Leistungskontrolle; die Möglichkeit, ständig beobachtet zu werden; die Möglichkeit des Arbeitgebers, die Kommunikationsdaten jederzeit einsehen zu können (vgl. Dahlbeck/Sobisch 2013).
Eine umfassende Gefährdungsanalyse, die auch die psychischen Belastungen umfasst, ist ein probates Mittel, um Gesundheitsgefährdungen für die Beschäftigten zu erkennen. Wenn sogar die Nutzung von mobilen Geräten in Frage gestellt werden kann, zeigt das einen hohen Grad an Problembewusstsein bei den Beteiligten.

„Die [Firma] führt eine regelmäßige Gefährdungsanalyse mindestens im Abstand von zwei Jahren durch. Die Gefährdungsanalyse erfolgt erstmals zum Ablauf der Probephase. Ergeben sich dabei eine erhöhte Stressbelastung oder andere Belastungsfaktoren der Beschäftigten, wird die [Firma] unverzüglich gemeinsam mit dem BR darüber verhandeln, ob oder in welcher Form eine Weiternutzung der mobilen Endgeräte fortgeführt wird."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Die folgende Regelung sieht das Gefährdungspotenzial insbesondere in den Aspekten Verfügbarkeit, Erreichbarkeit, Erholung. Daher ließen sich durch MDM Grenzen ziehen, indem die dienstlichen Mails und Aufgaben außerhalb bestimmter Zeiten nicht mehr zur Verfügung gestellt werden.

„Es besteht Einigkeit darüber, dass anlässlich der Einführung von iPads auch Gesundheitsaspekte nicht unberücksichtigt bleiben dürfen, insbesondere unter dem Aspekt Verfügbarkeit/Erreichbarkeit/Erholung usw. Es wird daher vereinbart, dass spätestens ein Jahr nach Inkrafttreten dieser Gesamtbetriebsvereinbarung die dann vorliegenden Erfahrungen ausgewertet werden. Sollte Regelungsbedarf erkannt werden, so wird im Rahmen der bestehenden Mitbestimmungsrechte hierüber verhandelt."

CHEMISCHE INDUSTRIE, 050340/39/2012

Dazu wurde nachstehend auch die Softwareergonomie bedacht, die insbesondere den kleinen Bildschirmen der mobilen Geräte angepasst werden sollte.

> „Aus Gründen des Gesundheitsschutzes werden nur Geräte oder Systeme eingesetzt, die dem aktuellen Stand arbeitswissenschaftlicher und software-ergonomischer Erkenntnisse entsprechen und die Normen der Reihe ISO 9241 erfüllen."
>
> KREDITGEWERBE, 090202/220/2012

2.9 Haftung für Verlust, Reparatur

Die MDM-Systeme können permanent kontrollieren, was mit den Geräten und den darauf befindlichen Daten geschieht, wo diese sich befinden und wer sie nutzt. Einerseits besteht bei den kleinen mobilen Geräten das Risiko, dass sie verloren, liegen gelassen oder gestohlen werden. Andererseits besteht hinsichtlich der Daten die Gefahr, dass Dritte sich widerrechtlich Zugang verschaffen, Viren oder andere Schadsoftware versehentlich auf das Gerät geladen werden. In diesen Fällen stellt sich die Frage: Wer haftet für einen Schaden?
Nach den schon vor Jahren vom Bundesarbeitsgericht entwickelten Grundsätzen gilt die Beschränkung der Arbeitnehmerhaftung für alle Beschäftigten (BAG vom 27.09.1994, Az.: GS 1/89) in folgendem Umfang:

- Sie haften bei vorsätzlich verursachten Schäden in vollem Umfang (BAG vom 25.09.1997, Az.: 8 AZR 288/96),
- bei leichtester Fahrlässigkeit haften sie dagegen nicht.
- Bei normaler Fahrlässigkeit ist der Schaden in aller Regel zwischen Beschäftigten und Arbeitgeber zu verteilen,
- bei grober Fahrlässigkeit hat die bzw. der Beschäftigte in aller Regel den gesamten Schaden zu tragen, der allerdings nicht in einem Missverhältnis zum Einkommend der Beschäftigten stehen darf (BAG vom 12.11.1998, Az.: 8 AZR 221/97 zur Haftungsobergrenze von drei Monatseinkommen).

Hinzu kommen jedoch Haftungserleichterungen, die von einer Abwägung im Einzelfall abhängen. Dabei sind insbesondere Schadensanlass, Schadensfolgen, Billigkeits- und Zumutbarkeitsgesichtspunkte zu bewerten: Eine möglicherweise vorliegende Gefahrgeneigtheit der Arbeit ist ebenso zu berücksichtigen wie die Schadenshöhe, ein vom Arbeitgeber einkalkuliertes Risiko, eine Risikodeckung durch eine Versicherung, die Stellung der/des Beschäftigten im Betrieb und die Höhe der Vergütung, die möglicherweise eine Risikoprämie enthalten kann. Auch die persönlichen Verhältnisse der bzw. des Beschäftigten sowie die Umstände des Arbeitsverhältnisses können zu berücksichtigen sein: beispielsweise ihr bzw. sein bisheriges Verhalten, die Dauer der Betriebszugehörigkeit, das Lebensalter, die Familienverhältnisse. Nach § 619a BGB muss der Arbeitgeber darlegen und beweisen, dass die bzw. der Beschäftigte vorwerfbar ihre bzw. seine Pflichten aus dem Arbeitsvertrag verletzt hat und nach § 280 Abs. 1 BGB zum Schadensersatz verpflichtet ist.
Keine Antwort auf die schwierigen Wertungsfragen der Haftung gibt die nachstehende Bestimmung. Sie verweist auf die Grundsätze der Arbeitnehmerhaftung und gibt damit vor, dies wäre Allgemeinwissen und allen Beschäftigten klar. Wann konkret ein Haftungsfall eintreten kann, bleibt für die meisten Beschäftigten damit im Dunkeln.

„Die Mitarbeiter haben das mobile IuK-Gerät sorgfältig zu behandeln. Für Beschädigung, Zerstörung und Diebstahl haften die Mitarbeiter bei Vorsatz und grober Fahrlässigkeit unter Anwendung der Grundsätze der Arbeitnehmerhaftung sowie der Beweislastregel des § 619a BGB."

GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

2.9.1 Haftung der Beschäftigten

Den beschriebenen schwierigen Bewertungsfragen für eine tatsächliche Haftung der Beschäftigten geht die folgende Regelung aus dem Weg: Sie stellt die Beschäftigten gänzlich frei von der Haftung bei Verlust oder Beschädigungen, die nicht vorsätzlich herbeigeführt wurden. Entsteht den Beschäftigten ein Schaden aus den drei genannten Gründen, haftet die Firma. Erstmalig wird hier das Schadensrisiko der Beschäftigten thematisiert.

„Hat der/die Beschäftigte den Schaden vorsätzlich verursacht, hat er/sie die Kosten der Reparatur zu tragen; in allen anderen Fällen trägt die Kosten die (Firma). Die Beschäftigten haften nur für vorsätzliches Handeln. Dies gilt sowohl für den Verlust als auch die Beschädigung des mobilen Endgerätes.
Entsteht dem/der Beschäftigten aufgrund missbräuchlicher Nutzung personenbezogener oder privater Daten wegen fehlenden Schutzes vor missbräuchlichen Zugriffen Dritter oder wegen des untersagten Auswertens von Daten ein Schaden, so haftet die [Firma] vollumfänglich im Rahmen eines Schadensersatzanspruchs."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Keine Antwort auf die Frage der Haftung der Beschäftigten gibt eine Regelung, die sich nur mit dem Löschen der Daten beschäftigt. Sie verdeutlicht den Betroffenen auch nicht, welche Risiken sie übernehmen, wenn sie mit mobilen Geräten arbeiten.

„Bei einem Verlust des mobilen IuK-Gerätes ist unverzüglich der zuständige Systemadministrator zu informieren, damit möglichst schnell aus Gründen der Missbrauchsprävention alle auf dem mobilen IuK-Gerät gespeicherten Daten mittels Fernsteuerung gelöscht werden können."

GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Nachstehend wird die Haftung auf rein vorsätzliches Handeln reduziert. Vorsätzlich bedeutet mit Wissen und Wollen zu handeln. Beispiel: Ein Mitarbeiter ärgert sich über sein Smartphone, weil es schon wieder abgestürzt ist, und wirft es mit aller Kraft gegen die Wand. Den entstehenden Schaden muss er tragen, da er vorsätzlich das Gerät zerstören wollte.

„Die Beschäftigten haften nur für vorsätzliches Handeln. Dies gilt sowohl für den Verlust als auch die Beschädigung des mobilen Endgerätes."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Mit der folgenden Regelung wird die Haftung für privaten Gebrauch auf vorsätzliches oder grob fahrlässiges Handeln beschränkt. Damit ist wahrscheinlich gemeint, dass die Haftungsgrundsätze für Beschäftigte (vgl. Kap. 2.9) für berufliche und private Nutzung Anwendung finden sollen. Beispiel für grobe Fahrlässigkeit: Eine Mitarbeiterin wirft ihr Smartphone der Kollegin zu, damit diese sich etwas anschaut. Dabei fällt es zu Boden und wird beschädigt.

„Die Haftung des Mitarbeiters im Rahmen der privaten Nutzung ist auf grobe Fahrlässigkeit und Vorsatz beschränkt."

CHEMISCHE INDUSTRIE, 050340/39/2012

Schließlich kann noch die Frage aufkommen: Haften Familien- oder Haushaltsangehörige ebenso, wie die Beschäftigten selbst? Gemäß der nachstehenden Lösung ist eine Einbeziehung möglich. Die Betriebsvereinbarung entfaltet ihre Wirksamkeit aber nur für die Beschäftigten im Betrieb. Eine Regelung zulasten Dritter ist rechtlich nicht möglich. In der Praxis entstünde eine sogenannte Haftungskette: Die Beschäftigten müssen sich für den Schaden gegenüber dem Arbeitgeber verantworten und können möglicherweise die bzw. den Schadensverursachenden in Regress nehmen.

„Im Falle der Beschädigung von [Firmen]-eigenen Arbeitsmitteln – einschließlich deren Verlustes bzw. des Verlustes von Datenbeständen – haften die Beschäftigten (einschließlich Haushaltsangehörige oder berechtigt in der Wohnung befindliche Dritte) nur, wenn die Beschädigung bzw. der Datenverlust vorsätzlich oder grob fahrlässig verursacht wurde."

ÖFFENTLICHE VERWALTUNG, 080102/223/2013

2.9.2 Wartung oder Reparatur der Geräte

Ein weiteres Problem kann entstehen, wenn ein mobiles Gerät zur Reparatur muss. Wenngleich die Beschäftigten ihre eigenen Geräte für dienstliche Zwecke nutzen dürfen, können sie mit ihnen nicht völlig frei verfahren. Sie müssen beachten, dass sich auf dem Gerät sensible Unternehmensdaten befinden können. Folgerichtig verpflichtet die nachstehende Regelung die Beschäftigten dazu, die Unternehmensdaten vor der Reparatur zu löschen.

„Auf dem mobilen Endgerät können u. U. sensible Unternehmensdaten gespeichert werden. Bei einem Defekt des Geräts können die Daten ggf. durch den Reparaturbetrieb eingesehen werden. Daher müssen die Daten vor der Reparatur gelöscht werden. Ist dies nicht mehr möglich, muss die Vertraulichkeit der gespeicherten Daten bewertet werden. Sind vertrauliche Unternehmensdaten gespeichert, darf das Gerät nicht repariert werden."

VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Es besteht das Risiko, dass Beschäftigte vor einer Reparatur versehentlich die Unternehmensdaten nicht löschen bzw. nicht gänzlich löschen. Dies umgeht die folgende Bestimmung, indem sie grundsätzlich eine durch den Arbeitgeber veranlasste Reparatur vorsieht. Nur in Ausnahmefällen sind die Beschäftigten berechtigt, die Reparatur durch Werkstätten vornehmen zu lassen, die dem Arbeitgeber fremd sind.

„In berechtigten Ausnahmefällen sind die Beschäftigten dazu berechtigt, eine Werkstatt auszuwählen und die Reparatur dort vornehmen zu lassen. Ein berechtigter Ausnahmefall liegt etwa vor, wenn der/die Beschäftigte auf die Nutzung des mobilen Endgerätes dringend angewiesen ist und sich räumlich weit von der [Firma] aufhält."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

2.9.3 Private Daten bei Verlust oder Reparatur

Soweit eine private Nutzung dienstlich überlassener Geräte erlaubt ist oder private Geräte dienstlich genutzt werden dürfen, werden in der Regel auf dem Gerät private Daten gesammelt. Diese gehen verloren, wenn das Gerät gestohlen wird oder wenn per Fernzugriff alle Daten über MDM gelöscht werden. Daher wird den Beschäftigten nachstehend geraten, eine Sicherung ihrer privaten Daten selbst zu veranlassen. Ihnen wird zwar das Recht eingeräumt zu wählen, ob im Falle eines Verlusts auch private Daten gelöscht werden sollen. Dies birgt jedoch das Risiko des widerrechtlichen Zugriffs durch nicht berechtigte Dritte. In der Praxis wäre noch zu beantworten, wie das MDM-System zwischen betrieblichen und privaten Daten unterscheidet.

> „Die Arbeitnehmer werden darauf hingewiesen, dass […] die technische Möglichkeit besteht – insbesondere im Falle des Verlusts des iPads – sämtliche auf dem iPad vorhandenen Daten, Anwendungen usw. per Fernzugriff zu löschen. Dem Mitarbeiter wird daher angeraten, selbst für eine ausreichende Backup-Sicherung für seine private Daten, Anwendungen usw. Sorge zu tragen. Der Mitarbeiter kann entscheiden, ob im Falle eines Verlustes des iPads neben den dienstlichen Funktionen auch private Daten, Anwendungen etc. gelöscht werden sollen."
>
> CHEMISCHE INDUSTRIE, 050340/39/2012

Die folgende Regelung sieht vor, dass eine längere Trennung vom MDM eine Sperrung der mobilen Geräte nach sich zieht. Damit ist gegebenenfalls auch die private Nutzung beeinträchtigt. Deshalb sollte vorher zumindest ein Hinweis erfolgen.

> „Endgeräte, die 60 Tage oder länger nicht mit dem MDM verbunden waren, werden automatisch gesperrt. Mit ihnen kann dann nicht mehr auf das [Firmen]-Netz zugegriffen werden."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Der Arbeitgeber kann die Geräte, die er den Beschäftigten als Arbeitsgeräte überlassen hat, für Überprüfungszwecke einziehen. Dies wird in nachstehender Regelung deutlich: Sie räumt die Möglichkeit einer Revision ein. Auch in diesem Fall hat der Arbeitgeber Zugriff auf die privaten Daten der Beschäftigten, wenn diese die Geräte auch privat nutzen dürfen. Laut Regelung darf der Arbeitgeber „jederzeit" zugreifen und die Geräte müssen „unmittelbar" ausgehändigt werden. Daher haben die Betroffenen möglicherweise keine Chance, ihre privaten Daten zu sichern oder wirksam zu löschen. Auch hier wäre eine Ankündigung sicher sinnvoll.

> „Der Arbeitgeber ist jederzeit zu einer Revision des mobilen IuK-Gerätes berechtigt. Zu diesem Zweck hat der Mitarbeiter dem Arbeitgeber das mobile IuK-Gerät unmittelbar nach Aufforderung auszuhändigen."
>
> GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Die vorstehenden Überlegungen und erörterten Problemen mit den privaten Daten auf dienstlichen Geräten und bei der Datensicherung durch MDM-Systeme ergeben folgende Konsequenz: Ein wirksamer Schutz bedeutet die Trennung von beruflichen und privaten Geräten. Nur wenn dienstlich überlassene Geräte nicht privat genutzt werden, können dort keine Daten anfallen, die den Arbeitgeber nichts angehen und die die Beschäftigten ihm nicht überlassen möchten.

2.10 Arbeitsrechtliche Sanktionen

Die Angst vor Verlust von Unternehmensdaten, vor Angriffen durch Schadsoftware und vor der Überwindung der „MDM-Mauer“ durch fehlerhaftes Verhalten der Beschäftigten führt in vielen Vereinbarungen dazu, dass den Beschäftigten arbeitsrechtliche Sanktionen angedroht werden. Gemäß der folgenden Vereinbarung müssen sich die Beschäftigten zu ihrer Einhaltung verpflichten. Damit wird eine ausdrückliche Erklärung der Beschäftigten nötig. Der Arbeitgeber kann bei jeglichen Verstößen gegen die Nutzungsvereinbarung arbeitsrechtliche Sanktionen aussprechen – eine sehr weitgehende Regelung.

> „Der Mitarbeiter verpflichtet sich, diese Vereinbarung einzuhalten. Verändert der Mitarbeiter vorsätzlich oder grob fahrlässig die genannten Einstellungen oder verstößt er in anderer Form gegen diese Nutzungsvereinbarung, behält sich das Unternehmen vor, arbeitsrechtliche Schritte gegen den Mitarbeiter einzuleiten.“
>
> FAHRZEUGHERSTELLER KRAFTWAGEN, 090202/203/0

Die nachfolgende Bestimmung stellt auf eine „betriebsübliche Sorgfalt“ ab. Solange diese eingehalten wird, müssen die Beschäftigten keine Sanktion fürchten. Wird an anderer Stelle genau und nachvollziehbar erklärt wird, was das für die Beschäftigten konkret bedeutet, wird damit der Rechtsprechung hinsichtlich möglicher Abmahnungen Rechnung getragen. Zu prüfen bleibt, ob letztlich das MDM-System mit seinem Schutz vor Viren und Trojanern versagt hat oder ob die Beschäftigten Fehler begangen haben.

> „Infiziert ein Beschäftigter die Systeme durch öffnen einer E-Mail oder durch den Aufruf einer Website oder wird sein Passwort ausgespäht, wird dies bei Einhaltung der betriebsüblichen Sorgfalt nicht geahndet.“
>
> KREDITGEWERBE, 090202/220/2012

Eine weitgehend dem Arbeitgeber überlassene Wertung ergibt sich aus nachfolgender Position. Die Begriffe Vorsatz, Fahrlässigkeit oder Sorgfaltsverletzungen spielen keine Rolle. Hier ist es nicht gelungen, Mindestschutzräume für die Beschäftigten zu errichten.

> „Verletzungen dieser Richtlinie können zu Disziplinarmaßnahmen bis hin zur Beendigung des Arbeitsverhältnisses führen.“
>
> CHEMISCHE INDUSTRIE, 090202/190/2012

Eine Art Sanktion für den Arbeitgeber stellt die folgende Vereinbarung dar, die unzulässiges Verhalten seitens des Arbeitgebers thematisiert. Danach besteht ein Auswertungs- und Verwertungsverbot für Informationen, die der Arbeitgeber erlangt, indem er gegen die Vereinbarung verstößt.

> „Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieser Betriebsvereinbarung gewonnen werden, sind unwirksam. Erkenntnisse aus solchen Informationen dürfen weder bei internen Beurteilungen noch bei arbeitsgerichtlichen Verfahren als Beweismittel verwendet werden.“
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

2.11 Beteiligung BR/PR

Nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“ finden sich in fast allen Vereinbarungen Regelungen zur Beteiligung der Interessenvertretungen. Nachstehend hat der Betriebsrat

das Recht, jederzeit Informationen über die durchgeführten Maßnahmen anzufordern. Aber er hat selbst keinen Zugriff auf das MDM-System und kann nicht spontan jederzeit kontrollieren, ob die Regeln der Betriebsvereinbarung eingehalten werden.

> „Informationen über die durchgeführten Maßnahmen werden dem Betriebsrat jederzeit zur Verfügung gestellt."
>
> NACHRICHTENTECHNIK/UNTERHALTUNGS-, AUTOMOBILELEKTRONIK, 090202/208/2013

Die folgende Bestimmung ermöglicht dem Betriebsrat eine Information und bei Mitarbeiterkontrollen eine Beteiligung. Dies spiegelt seine Funktion gemäß BetrVG wider, wonach er den Beschäftigten auch zur Seite steht. Der letzte Satz geht über die Möglichkeiten des BetrVG hinaus: Er lässt nur mit „Zustimmung" des Betriebsrates eine über den abrechnungsbezogenen Missbrauchsverdacht hinausgehende Kontrolle der mobilen Geräte der Beschäftigten zu.

> „Sollte durch die Höhe der Providerrechnung ein Missbrauchsverdacht vorliegen, ist der Betriebsrat darüber umgehend zu informieren, um im Anschluss daran den Gründen für die hohen Kosten nachzugehen; eine darüber hinausgehende Kontrolle der Mitarbeiter bzgl. des Einsatzes von Smartphones bedarf der vorherigen Zustimmung des BR."
>
> LEASINGUNTERNEHMEN, 090202/196/2012

Mit der nachstehender Regelung wird der Betriebsrat informiert, muss aber selbst entscheiden, ob er ein Mitbestimmungsverfahren in Gang setzen möchte. Damit kann der Arbeitgeber die Black-List erst einmal verändern und der Betriebsrat nur im Nachhinein seine Beteiligung verlangen. Fraglich ist: Kann diese Beteiligung auch eine Änderung der Black-List nach sich ziehen?

> „Bei Veränderungen der Black-List erhält der Konzernbetriebsrat per E-Mail eine Information mit der aktualisierten Black-List, sodass er entscheiden kann, ob er das Mitbestimmungsverfahren in Gang setzt."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Alle denkbaren Kontrollmöglichkeiten werden dem Gesamtbetriebsrat im Folgenden eingeräumt, damit er prüfen kann, ob die vereinbarten Regeln durch das MDM-System eingehalten werden. Sehr sinnvoll ist es zudem, wenn die Interessenvertretung das Recht hat, sachverständige Unterstützung hinzuzuziehen. Sicher vermag nicht jede Betriebsrätin bzw. jeder Betriebsrat ein Softwaresystem so weit zu durchdringen, dass Einstellungen auf der Admin-Ebene deutlich werden.

> „Der GBR kann die Einhaltung dieser GBV jederzeit auf jede ihm geeignet erscheinende Weise überprüfen. Er kann zur Durchführung seiner aus dieser GBV resultierenden Aufgaben einen Sachverständigen seiner Wahl in Abstimmung mit der Bank hinzuziehen; die notwendigen Kosten trägt die Bank."
>
> KREDITGEWERBE, 090202/220/2012

Insgesamt deutet diese Regelung auf großes Vertrauen zwischen den Betriebsparteien hin. Alles wird transparent dargelegt; die Kosten übernimmt der Arbeitgeber, wenn eine Abstimmung mit ihm erfolgte. Das Unternehmen vertraut offensichtlich darauf, dass der Gesamtbetriebsrat mit dieser Möglichkeit verantwortungsvoll umgeht. Die Idee der vertrauensvollen Zusammenarbeit des § 2 BetrVG wird hier umgesetzt.

3 Mitbestimmungsrechte

Aufgrund unterschiedlicher Mitbestimmungstatbestände des Betriebsverfassungsgesetzes und der Personalvertretungsgesetze des Bundes und der Länder müssen die Interessenvertretungen beteiligt werden. Hinzu treten die Bestimmungen zum Schutz personenbezogener und schon personenbeziehbarer Daten der Beschäftigten nach dem Bundesdatenschutzgesetz und gegebenenfalls nach den Datenschutzgesetzen der Bundesländer.
Die MDM-Systeme wirken im Hintergrund. Sie sind nicht unbedingt für die Betroffenen erkennbar und können jederzeit zur Kontrolle der Beschäftigten eingesetzt werden: über die Kamera, das Mikrofon, ein Mithören oder GPS im mobilen Gerät. Daher greifen die Grundsatzaussagen des Bundesverwaltungsgerichtes (BVerwG vom 23.09.1992, Az.: 6 P 26/90) und des Bundesarbeitsgerichtes (BAG vom 14.09.1984, Az.: 1 ABR 23/82): Es reicht aus, dass die Beschäftigten befürchten müssen, während der Arbeit mithilfe technischer oder elektronischer Kontrolleinrichtungen jederzeit beobachtet oder in anderer Weise fortlaufend kontrolliert zu werden. Dieser entstehende Überwachungsdruck behindert sie in der freien Entfaltung ihrer Persönlichkeit. Hat das mobile Gerät beispielsweise eine Kamera, kann diese über MDM aktiviert und somit das Geschehen direkt beobachtet, gefilmt und ferngespeichert werden. Das Bundesarbeitsgericht entschied bereits 1987, dass eine lückenlose Aufzeichnung der Tätigkeiten der Beschäftigten durch Kameras unzulässig in ihre Persönlichkeitsrechte eingreift (BAG vom 7.10.1987, Az.: 5 AZR 116/86). Somit besteht für die Interessenvertretungen eine Hauptaufgabe darin, über Vereinbarungen im Unternehmen diesen Überwachungsdruck zu verhindern oder zumindest abzumildern.

3.1 Regelungen zu Verhalten und Ordnung im Betrieb

Gegenstand des Mitbestimmungsrechts (§ 87 Abs. 1 Nr. 1 BetrVG) ist das betriebliche Zusammenleben und Zusammenwirken der Beschäftigten. Reine Arbeitsanweisungen („Anrufe sind auf dem Formular XY zu notieren“) durch den Arbeitgeber sind mitbestimmungsfrei. Ebenso hat der Betriebsrat kein Mitbestimmungsrecht, wenn es um die private Lebensführung außerhalb des Betriebes geht (funktional und nicht räumlich zu verstehen). Denn diese ist – eigentlich – vom Unternehmen auch nicht regelbar (BAG vom 28.05.2002, Az.: 1 ABR 32/01). Demnach wäre die folgende Regelung als Arbeitsanweisung mitbestimmungsfrei.

> „Die Beschäftigten sind auf Aufforderung verpflichtet, dienstliche Daten von mobilen Endgeräten auf andere verfügbare dienstliche Geräte zu laden oder den Zugriff zu ermöglichen.“
>
> ÖFFENTLICHE VERWALTUNG, 090202/137/2009

Sobald Entscheidungsspielräume entstehen oder auch der private Bereich der Beschäftigten durch betriebliche Maßnahmen betroffen sein kann, setzt die Mitbestimmung ein. Denn der Betriebsrat hat die Aufgabe, darüber zu wachen, dass die Persönlichkeitsrechte der Beschäftigten nicht verletzt werden (BAG vom 18.04.2000, Az.: 1 ABR 22/99). Es handelt sich dabei um sogenannte Regelungen zum Verhalten der Beschäftigten oder der Ordnung im Betrieb (§ 87 Abs. 1 Ziff. 1 BetrVG). Gleiches gilt für die Personalräte gemäß § 75 Abs. 3 Ziff. 15 BPersVG.
In der Grundsatzentscheidung des BAG im Jahr 2008 zum „Code Of Business Conduct“ der Firma Honeywell wurde die Aufgabe der Interessenvertretung klar umrissen: Der Betriebsrat soll im Rahmen der Mitbestimmung darauf achten, dass durch die Regelung keine Persönlichkeitsrechte der Arbeitnehmer verletzt werden. Folglich sind Regelungen über im Betrieb stattfindende private Verhaltensweisen der Arbeitnehmer nicht generell mitbestimmungsfrei – insbesondere wenn es um das Verhältnis zwischen Vorgesetzten und Untergebenen geht (BAG vom 22.07.2008, Az. 1 ABR 40/07). Der Schutz der Persönlichkeitsrechte steht demnach im Vordergrund.

In der nachfolgender Bestimmung wird deutlich: Die Betriebsparteien haben erkannt, dass bei privater Nutzung immer Schutzregeln für die privaten Daten nötig sind.

> „Sofern ein Beschäftigter dienstliche IT-Systeme für private Zwecke nutzt, kann eine Kenntnisnahme der privaten Daten oder Informationen durch Dritte nicht ausgeschlossen werden. Vereinbarungen von Konzerngesellschaften, die eine private Nutzung dienstlicher IT-Systeme erlauben, müssen daher auch Regelungen zum Umgang mit privaten Daten und Informationen sowie zu deren Schutz treffen, etwa für den Fall einer längeren Abwesenheit des Beschäftigten oder für das Vorliegen des Verdachts auf eine strafbare Handlung."
>
> BERGBAU, 090201/531/2012

Auf die Form der Regelung kommt es nicht an. Der Mitbestimmung würden auch Richtlinien unterliegen. Sobald Regelungen geschaffen werden, die das Verhalten der Beschäftigten in Bezug auf die betriebliche Ordnung betreffen, ohne dass sie verbindliche Vorgaben zum Inhalt haben müssen, setzt das Mitbestimmungsrecht des Betriebsrates ein: „Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG setzt nicht notwendig voraus, dass es sich um verbindliche Verhaltensregeln handelt. Ausreichend ist es, wenn die Maßnahme darauf gerichtet ist, das Verhalten der Arbeitnehmer zu steuern oder die Ordnung des Betriebs zu gewährleisten" (BAG vom 18.04.2000, Az.: 1 ABR 22/99).
Die Mitbestimmung ist ausgeschlossen, wenn gesetzliche oder tarifliche Regelungen bestehen (§ 87 Abs. 1 BetrVG). Dies gilt jedoch nur, wenn es sich um eine abschließende Regelung handelt.

3.2 Arbeitszeit

Erkennbar sind in den ausgewerteten Vereinbarungen erste Ansätze, die ein Ausweiten der Arbeitszeit oder eine Rufbereitschaft „durch die Hintertür" verhindern sollen (vgl. Nies/Vogl 2013). Teilweise werden auch Fragen zur Bezahlung von Arbeitszeit außerhalb des Unternehmens angesprochen. Die Mitbestimmungsrechte des § 87 Abs. 1 Nr. 2 und 3 BetrVG und § 75 Abs. 3 Nr. 1 BPersVG gewähren den Betriebs- und Personalräten in diesem Bereich ein volles Beteiligungsrecht. Sie können initiativ tätig werden und neue Vereinbarungen verlangen. Über die vorgesehenen Einigungsstellen ist es möglich, Streitigkeiten abschließend beizulegen.
Über die MDM-Systeme lässt sich die Höchstdauer der täglichen oder wöchentlichen Arbeitszeit steuern. Pausenzeiten können kontrolliert und sogar erzwungen werden. Schließlich gilt zu bedenken, dass die Arbeit mit mobilen Geräten Mehrarbeit oder Überstunden darstellen kann und zu vergüten ist (Baunack 2014). Dies folgt aus europäischem Recht: Richtlinie Art. 2 Nr. 1 und 2 RL 93/104/EG bestimmt, dass es sich um Arbeitszeit handelt, wenn Beschäftigte Aufgaben aus ihrem Arbeitsverhältnis wahrnehmen – beispielsweise, wenn sie eine dienstliche Mail schreiben.
Die folgende Regelung wirkt einerseits dem Trend entgegen, immer und überall erreichbar sein zu müssen (von Lüpke 2013); andererseits schützt sich das Unternehmen vor Entgeltforderungen der Beschäftigten. Die berufliche Nutzung mobiler Geräte ist nur in der individuellen Arbeitszeit zulässig.

> „Die dienstliche Nutzung der von der [Firma] zur Verfügung gestellten mobilen Endgeräte erfolgt während der individuellen Arbeitszeit. In dieser Zeit hat der/die Beschäftigte über das mobile Endgerät für die [Firma] erreichbar zu sein."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Auch die nächste Regelung beschäftigt sich mit dem Anspruch eines Unternehmens, kein Entgelt leisten zu müssen, wenn die Beschäftigten außerhalb ihrer persönlichen Arbeitszeit arbeiten. Vor dem Grundgedanken europäischen Rechts ist diese Regelung unwirksam. Der individualrechtliche Entgeltanspruch kann nicht durch eine Betriebsvereinbarung beschnitten werden. Es gilt mindestens das Günstigkeitsprinzip: Demnach können die Beschäftigten für Arbeitszeit, die der Arbeitgeber entgegennimmt auch eine Bezahlung verlangen.

> „Besitz oder Nutzung des Tokens begründen für sich keinen Anspruch auf Anrechnung als Arbeitszeit. Die Frage, ob die Zeiten der Nutzung des Tokens als Dienst- oder Arbeitszeit zu bewerten sind, richtet sich nach der Dienstvereinbarung über die Regelung der täglichen Arbeitszeit. Die Nutzung außerhalb der Kernarbeitszeit beruht grundsätzlich auf dem Prinzip der Freiwilligkeit. Bei Dienstreisen gilt die Regelarbeitszeit. In Ausnahmefällen kann zwischen der/dem Vorgesetzten und der/dem Mitarbeiter/in die Nutzung des Token vereinbart werden, wenn damit eine zwingende Anwesenheitspflicht in der Dienststelle vermieden werden kann. Die Anrechnung der Arbeitszeit aufgrund dienstlicher Erfordernisse erfolgt in Absprache zwischen der/dem unmittelbaren Vorgesetzten und der/dem Beschäftigten. Die abgestimmte Arbeitszeit ist nachträglich als Korrektur zu erfassen und über den/die unmittelbare/n Vorgesetzte/n weiterzuleiten.“
>
> ÖFFENTLICHE VERWALTUNG, 080102/223/2013

Die Unternehmen haben es mit MDM auch in der Hand, die Arbeit außerhalb der persönlichen Arbeitszeit zu unterbinden. Nutzen sie diese Möglichkeit nicht, entspricht dies einer Form der Entgegennahme von Arbeit – was zu Entgeltansprüchen der Beschäftigten führt.
Besonders in Bereichen mit großem Termindruck und hohem Arbeitsaufkommen könnten sich die Beschäftigten einem erheblichen psychischen Druck ausgesetzt sehen, die dienstlichen mobilen Geräte außerhalb der Arbeitszeit zu nutzen und ständig für den Arbeitgeber erreichbar zu sein. Denn: Andere Kollegen tun dies gegebenenfalls auch. Viele Beschäftigte gehen davon aus, ein solches Verhalten wäre durch den Arbeitgeber ausdrücklich erwünscht.
Die Folge einer solch unkontrollierten Nutzung könnten Verstöße gegen das Arbeitszeitgesetz sein. Denkbar wäre insbesondere ein Verstoß gegen § 3 ArbZG (Werktägliche Arbeitszeit). Darüber hinaus wären auch Verstöße gegen § 5 ArbZG (Ruhezeit) möglich, etwa wenn Beschäftigte noch spät abends dienstliche E-Mails lesen und gegebenenfalls beantworten.
Schließlich ist das Unternehmen verpflichtet, eine über die werktägliche Arbeitszeit (in der Regel 8 Stunden) hinausgehende Arbeitszeit der Beschäftigten aufzuzeichnen (§ 16 Abs. 2 ArbZG).

3.3 Leistungs- und Verhaltenskontrolle

§ 87 Abs. 1 Nr. 6 BetrVG räumt dem Betriebsrat ein Mitbestimmungsrecht ein, bei „der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Diese Vorschrift verlangt keine Absicht, diese Kontrollen auszuführen. Das Mitbestimmungsrecht wird bereits ausgelöst, wenn die Einrichtung dazu geeignet ist, die Kontrolle zu ermöglichen.
Mit § 75 Abs. 3 Nr. 17 BPersVG besteht eine inhaltsgleiche Regelung für Personalräte. Das Bundesverwaltungsgericht unterscheidet hinsichtlich der Beteiligung des Personalrats nicht danach, ob die technische Einrichtung zur Überwachung geeignet oder bestimmt ist. Ein Beteiligungsrecht der Interessenvertretung wird von dem Gericht immer dann unterstellt, wenn die technische Einrichtung für einen Überwachungsvorgang eingesetzt werden kann (BVerwG vom 31.8.1988, AZ.: 6 P 21.86). In den Bundesländern ist dies teilweise anders (vgl. Kap. 6.3.3).
MDM kann die mobilen Geräte beobachten, indem es sich auf das Gerät aufschaltet. Es wird erkennbar, welche Anwendung gerade benutzt wird, welche Daten eingegeben werden und

so weiter. Hat das mobile Gerät eine Kamera, kann diese über MDM aktiviert und somit das Geschehen direkt beobachtet, gefilmt und ferngespeichert werden. Das Bundesarbeitsgericht entschied bereits 1987, dass eine lückenlose Aufzeichnung der Tätigkeiten der Beschäftigten durch Kameras unzulässig in ihre Persönlichkeitsrechte eingreift (BAG vom 7.10.1987, Az.: 5 AZR 116/86).
Das LAG Hamm geht einen Schritt weiter als das BAG. Ihm zufolge könnten auch zeitlich limitierte Filmaufnahmen das Persönlichkeitsrecht der Beschäftigten verletzen (LAG Hamm vom 30.12.2012, Az.: 9 Sa 158/12): „Soweit der Arbeitnehmer nicht weiß, wann eine Überwachungskamera an seinem Arbeitsplatz in Betrieb ist und er den genauen Erfassungsbereich nicht kennt, ist er in einem über die rein objektive Beobachtungszeit hinausgehenden Zeitraum dem Anpassungsdruck ausgesetzt, auch wenn dieser keineswegs während der jeweiligen vollen Arbeitsschicht vorliegt."
Die Möglichkeit der Überwachung reicht demnach aus. Eine mitbestimmungspflichtige technische Überwachungseinrichtung liegt bereits vor, wenn die Einrichtung es ermöglicht, das Verhalten oder die Leistung von Beschäftigten zu überwachen, ohne dass dies konkret gewollt oder installiert sein muss. In der folgenden Regelung wird folgerichtig auch ohne Einschränkung die Beteiligung des Betriebsrates vorgesehen.

> „Soweit die Gesellschaften zukünftig neue Systeme, IuK-Geräte, Programme/Apps oder sonstige Systeme der elektronischen Datenverarbeitung neu einführen, sind die Rechte des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG zu beachten."
>
> GRUNDSTÜCKS- UND WOHNUNGSWESEN, 090202/200/2013

Die nachstehende Regelung schließt das Aufschalten während einer „Benutzersitzung" aus, wenn die Beschäftigten nicht zustimmen. Mit Benutzersitzung ist wahrscheinlich die aktive Nutzung des mobilen Gerätes durch die bzw. den Beschäftigten gemeint. Damit wäre eine Beobachtung im Sinne von „immer und überall" (vgl. von Lüpke 2013) technisch möglich, aber unzulässig. Es stellt sich die Frage: Wie kann kontrolliert werden, dass diese Regelung eingehalten wird?

> „Zur Erreichung des genannten Zwecks kann sich ein Administrator bzw. Mitarbeiter mit besonderen Systemberechtigungen jederzeit – ggf. auch bei ausgeschaltetem Endgerät und ohne Mitwirkung des Anwenders – per Fernwartungssoftware auf das Endgerät schalten. In einer laufenden Benutzersitzung erfolgt die Aufschaltung jedoch nur nach Zustimmung des Anwenders. Eine darüber hinausgehende Aufzeichnung der Aufschaltungssitzung wird nur in Ausnahmefällen nach vorhergehender Vereinbarung zwischen Aufschaltendem und Anwender durchgeführt."
>
> BERGBAU, 090201/531/2012

Bei einer Überwachung durch ein Kamerasystem in den Arbeitsräumen ist es wichtig, dass die Beschäftigten sich der Überwachung entziehen können (vgl. Dahlbeck/Sobisch 2013). Auch eine Überwachung in Sozial- und Pausenräumen ist unzulässig. Bei den mobilen Geräten wird über MDM eine ständige Kontrolle und Auswertung möglich. Neben den Auswertungen sollten auch Kontrollen und Steuerungen über MDM geregelt werden.

> „Auswertungen sind nur zulässig, wenn der BR vorab zugestimmt hat."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

In der folgenden Regelung wird die Leistungskontrolle ausgeschlossen. Dies bedeutet im Umkehrschluss: Eine Verhaltenskontrolle ist nicht geregelt. Dies ist jedoch kein Freibrief für die Dienststelle, sondern erfordert für jede Verhaltenskontrolle oder -auswertung, dass vorher ein Mitbestimmungsverfahren durchgeführt wird.

„Die mit Hilfe der mobilen Erfassungsgeräte gespeicherten Daten dürfen grundsätzlich nicht zur individuellen Leistungskontrolle der Mitarbeiter/innen verwendet werden. Ausnahmen sind nur mit vorheriger Zustimmung der betroffenen Mitarbeiter/innen und der Personalvertretung zulässig."

ÖFFENTLICHE VERWALTUNG, 090202/199/2012

MDM-Systeme mit der Möglichkeit der Remote Control oder Fernsteuerung lassen direkte Zugriffe auf die mobilen Geräte zu. Dieses Aufschalten sollte untersagt oder zumindest begrenzt werden. Denn es würde zu einer permanenten Überwachung der Beschäftigten führen. Eine Kontrolle ist ebenfalls sehr schwierig, da ein Aufschalten möglicherweise nicht protokolliert wird und daher nicht nachvollziehbar ist.

3.4 Datenschutz

Das Datenschutzrecht ist als Verbot mit einem sogenannten Erlaubnisvorbehalt konzipiert (§ 4 BDSG). Personenbezogenen Daten dürfen demnach grundsätzlich nicht erhoben, gespeichert oder verarbeitet werden, wenn a) dies nicht entweder durch eine (gesetzliche) Vorschrift ausdrücklich erlaubt ist oder b) der jeweilige Betroffene der jeweiligen Datennutzung nicht ausdrücklich zugestimmt hat. Das Bundesdatenschutzgesetz (§ 3a) formuliert für den Umgang mit personenbezogenen Daten außerdem den Grundsatz der Datensparsamkeit.
Auch für das Beschäftigungsverhältnis gilt: Nicht einfach alle anfallenden personenbezogenen Daten dürfen vom Unternehmen genutzt werden. Dies ist grundsätzlich nur im Rahmen des § 32 BDSG zulässig: „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."
MDM erfasst personenbezogene Daten, die nicht zur Begründung oder für die Durchführung des Beschäftigungsverhältnisses notwendig sind. Deshalb müssen entweder die Betroffenen zustimmen oder eine Betriebsvereinbarung dient als Rechtsvorschrift im Sinne des § 4 BDSG für die Erhebung, Speicherung und Verarbeitung der Daten. Soweit private Daten der Beschäftigten, ihr Aufenthaltsort, E-Mail-Inhalte und private Adressen betroffen sind, handelt es sich um besonders sensible Daten im Sinne von § 3 Abs. 9 BDSG. Für sie sind nach § 4a Abs. 3, § 28 Abs. 6 bis Abs. 9 BDSG erhöhte Anforderungen an die Erhebung und Speicherung zu stellen (BAG vom 23. August 2012 – 8 AZR 804/11). Daher wird für diesen Fall auch weiterhin eine ausdrückliche Einwilligung der Beschäftigten nach § 4a BDSG erforderlich sein (Däubler et al. 2013, § 32 Rn. 10). In der folgenden Bestimmung wird auf die gesetzlichen Regelungen verwiesen, ohne die entsprechende Konsequenz einer persönlichen Einwilligung zu fordern.

„Die gesetzlichen Anforderungen an die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten sowie etwaige gesetzliche Informationspflichten sind zu beachten. Im Übrigen finden die Begriffsbestimmungen des Bundesdatenschutzgesetzes auf diese Konzernbetriebsvereinbarung Anwendung, soweit sich aus dieser Konzernbetriebsvereinbarung nicht ausdrücklich etwas anderes ergibt."

BERGBAU, 090201/531/2012

Das Bundesverfassungsgericht hat in den vergangenen Jahren den Schutz der Persönlichkeit herausgestellt. Es betonte im Jahr 2008, dass das allgemeine Persönlichkeitsrecht in Art. 2 Abs. 1 und Art. 1 Abs. 1 GG das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst (BVerfG vom 27.2.2008, Az.: 1 BvR 370/07). Der Grundgedanke ist der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten sowie die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu be-

stimmen (BVerfG vom 15.12.1983, Az.: 1 BvR 209/83). Der Betriebsrat ist daher hinsichtlich der folgenden Fragen zu beteiligen:

- Welche Daten der Beschäftigten dürfen überhaupt erfasst und gespeichert werden?
- Wie dürfen diese Daten verwendet werden?
- Wie dürfen sie verknüpft und ausgewertet werden?

Der Schutz der Persönlichkeitsrechte der Beschäftigten ist dabei das zentrale Ziel.
Dies gilt auch für Personalräte, obwohl der Datenschutz in § 68 BPersVG nicht ausdrücklich als Aufgabe des Personalrats erwähnt ist. Aber nach § 68 Abs. 1 Nr. 2 BPersVG hat die Personalvertretung darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Gesetze von der Dienststelle durchgeführt werden. Ein direktes Mitbestimmungsrecht zum Datenschutz findet sich im BPersVG nicht. In den Bundesländern dagegen bestehen größtenteils ausdrückliche Mitbestimmungsrechte bei der Festlegung oder Veränderung des Umfangs der Verarbeitung personenbezogener Daten der Beschäftigten.
Insbesondere haben die Betriebsparteien zu beachten: Private Daten sind besonders geschützt und auch ein Verbot privater E-Mails stellt kein Freibrief für den Arbeitgeber dar, jederzeit Einsicht zu nehmen in die Daten der Beschäftigten (vgl. Rozeck 2014). Die Regelung in einer Betriebsvereinbarung ist sinnvoll und erforderlich. Dabei sollten die Unternehmen auch die Verantwortung übernehmen und für den Schutz der privaten Daten sorgen.

> „Sofern ein Beschäftigter dienstliche IT-Systeme für private Zwecke nutzt, kann eine Kenntnisnahme der privaten Daten oder Informationen durch Dritte nicht ausgeschlossen werden. Vereinbarungen von Konzerngesellschaften, die eine private Nutzung dienstlicher IT-Systeme erlauben, müssen daher auch Regelungen zum Umgang mit privaten Daten und Informationen sowie zu deren Schutz treffen, etwa für den Fall einer längeren Abwesenheit des Beschäftigten oder für das Vorliegen des Verdachts auf eine strafbare Handlung."
>
> BERGBAU, 090201/531/2012

3.5 Qualifizierung

In vielen Vereinbarungen steht: Die Beschäftigten hätten die einschlägigen Datenschutzgesetze, strafrechtliche Bestimmungen und andere Gesetze einzuhalten. Allerdings wird nicht erklärt, was das in der Praxis konkret bedeutet. Um derartige Regelungen einhalten zu können, müssen die Beschäftigten über die Probleme und Risiken bei der Nutzung von mobilen Geräten und dem Web aufgeklärt werden. Ziel von Schulungs- und Bildungsmaßnahmen im betrieblichen Rahmen muss insbesondere sein, dass die Beschäftigten genau wissen, was sie im Netz tun, was sie über sich oder das Unternehmen preisgeben bzw. was sie besser nicht tun und kommunizieren sollten (vgl. Schwemme/Wedde 2012). Aber auch über die Risiken bei der Nutzung von Angeboten mobiler Arbeit im Sinne von unendlicher Freiheit einerseits und die Folgen übergroßer Selbstausbeutung andererseits müssen die Beschäftigten aufgeklärt sein. Derartige Schulungsinhalte kann der Betriebsrat gemäß § 96 BetrVG und der Personalrat gemäß § 75 Abs. 3 Ziff. 6 BPersVG dem Arbeitgeber vorschlagen. Hinsichtlich der Auswahl der Teilnehmerinnen und Teilnehmer steht ihm gemäß § 98 Abs. 3 BetrVG und dem Personalrat gemäß § 75 Abs. 3 Ziff. 7 BPersVG ein Mitentscheidungsrecht zu. Können sich die Parteien nicht einigen, entscheidet gemäß § 98 Abs. 4 BetrVG bei den Betriebsräten die Einigungsstelle. Diese Mitbestimmungsrechte werden in der folgenden Regelung bestärkt und konkretisiert.

„Der BR ist hinsichtlich etwaiger Auswirkungen auf die Arbeitszeit und den Gesundheitsschutz der Beschäftigten sowie in Bezug auf eine geplante Qualifizierungsmaßnahmen im Zusammenhang mit der Nutzung des MDM-Systems im Rahmen ihrer Mitbestimmungsrechte aus dem BetrVG zu beteiligen."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Eher einer Aufgabe der Mitbestimmungsrechte kommt die folgende Bestimmung nah. Denn sie überlässt es dem Arbeitgeber, den erforderlichen Schulungsumfang und -inhalt festzulegen.

„Der AG [Arbeitgeber] wird die von der Einführung betroffenen Mitarbeiter im erforderlichen Umfang schulen. Dabei können u. a. auch Schulungen im Rahmen des ‚e-learning' in Betracht kommen. Die möglichen Qualifizierungsmaßnahmen finden während der Arbeitszeit statt. Im Übrigen bleiben die Regelungen des § 98 BetrVG unberührt."

LEASINGUNTERNEHMEN, 090202/196/2012

Bei MDM-Systemen und mobilen Endgeräten handelt es sich um Arbeitsmittel, deren Einführung die bisherigen Arbeitsabläufe stark verändern kann. Ein Beschäftigter im Außendienst nimmt heute beispielsweise mit Tablet oder Notebook und Mini-Drucker ein komplettes Büro mit zum Kunden. Dort kann beispielsweise der Versicherungsvertrag sofort ausgedruckt werden. In solchen Fällen, wenn sich auch die Tätigkeit der Beschäftigten ändert, unterliegt die „Einführung von Maßnahmen" zur Qualifizierung der Mitbestimmung (§ 97 Abs. 2 BetrVG, § 75 Abs. 2 Ziff. 6 BPersVG).

3.6 Arbeits- und Gesundheitsschutz

Die Spannbreite der Fragen hinsichtlich des Gesundheitsschutzes reicht von einer gesundheitlichen Gefährdung durch Strahlen bis zur ergonomischen Gestaltung von Bildschirmen und Software auf mobilen Geräten. Diese Fragen zu stellen ist Aufgabe der Betriebsräte gemäß § 87 Abs. 1 Ziff. 7 und § 81 BetrVG sowie der Personalräte gemäß § 75 Abs. 3 Ziff. 11 und § 81 BPersVG. Diese Aufgabe umfasst das Ziel, nicht nur physische, sondern auch psychische Beanspruchungen zu vermeiden, in jedem Fall aber zu minimieren (LAG Hamm vom 09.03.2012, Az.: 13 TaBV 100/10).
Die Schutzmaßnahmen der §§ 9, 10 und 12 des Arbeitsschutzgesetzes betreffen nicht nur den Produktions-, sondern auch den Dienstleistungsbereich. Dazu gehören auch entsprechende Gefährdungsanalysen. Die konkreten arbeitsplatz- oder aufgabenbezogenen Unterweisungen sind an den Erkenntnissen der Gefährdungsanalyse im Sinne von § 5 ArbSchG auszurichten. Diesen Aspekt nimmt die folgende Regelung auf. Sie ermittelt im Rahmen einer Gefährdungsanalyse, welche Gefahren vorliegen.

„Der BR ist über die Ergebnisse der Gefährdungsanalysen unverzüglich zu unterrichten."

DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Bisher nicht ausreichend geregelt sind in den Vereinbarungen Fragen zur Ergonomie der mobilen Geräte und der Software auf den Geräten. Sie betreffen insbesondere Geräte mit kleinen Bildschirmen, mit denen E-Mails und andere Anwendungen bearbeitet werden. Gesundheitsschutz hinsichtlich Strahlungsrisiken wird zwar durchaus thematisiert; nicht jedoch der Schutz vor Überlastungen (insbesondere der Augen), Verspannungen oder Haltungsschäden. Je mehr mit den kleinen mobilen Geräten tatsächlich gearbeitet wird, desto stärker sollte die Interessenvertretung auf die Einhaltung ergonomischer Mindeststandards drängen. Die jahrelangen Auseinandersetzungen um die richtige Bildschirmgröße, die richtige Ausrichtung und Höhe sollten nicht mit mobilen Geräten unterlaufen werden dürfen (vgl. Klein 2013).

Gesundheit umfasst die körperliche und psychische Unversehrtheit. Dies wird bisher nur in wenigen Vereinbarungen problematisiert. Gefährdungen durch die Geräte selbst, ergonomische Mindestanforderungen und Sicherheitsansprüche sind bisher kaum in Vereinbarungen zu finden. Hinsichtlich möglicher psychischer Belastungen finden sich nur wenige Bestimmungen zur Stressvermeidung. Ebenso fehlt eine Auseinandersetzung mit dem Ausdehnen der beruflichen Belange in die Freizeit durch ständige Erreichbarkeit oder Sichtbarkeit von beruflichen Anforderungen (zum Beispiel E-Mails) und deren belastenden Folgen wie etwa psychische oder psychosomatische Erkrankungen (vgl. Baunack 2014).
In der nachstehenden Bestimmung wird zumindest schon der mögliche Stress erwähnt; er soll Teil einer Gefährdungsanalyse sein.

> „Die [Firma] führt eine regelmäßige Gefährdungsanalyse mindestens im Abstand von zwei Jahren durch. Die Gefährdungsanalyse erfolgt erstmals zum Ablauf der Probephase. Ergeben sich dabei eine erhöhte Stressbelastung oder andere Belastungsfaktoren der Beschäftigten, wird die [Firma] unverzüglich gemeinsam mit dem BR darüber verhandeln, ob oder in welcher Form eine Weiternutzung der mobilen Endgeräte fortgeführt wird."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Trotz Langzeittests ist immer noch unklar: Inwieweit gefährden mobiles Telefonieren und Tragen des Geräts am Körper die Gesundheit? Daher ist Vorsicht geboten. Die Aufklärungspflichten des Arbeitgebers (§ 81 Abs. 1 BetrVG) werden in der Praxis kaum realisiert. Hierzu gehört auch die durch § 12 ArbSchG dem Arbeitgeber auferlegte Verpflichtung, die Beschäftigten über Sicherheit und Gesundheitsschutz bei der Arbeit zu unterweisen. Einigen sich die Betriebsparteien nicht über Art und Inhalt der Unterweisung, ist gemäß § 76 BetrVG eine Einigungsstelle zu bilden, um den Streit beizulegen (BAG vom 11.1.2011, Az.: 1 ABR 104/09). Für Personalräte ist in diesem Bereich jedoch die Rechtslage anders. Das höchste deutsche Verwaltungsgericht lehnte im Jahr 2002 die Mitbestimmung eines Personalrats bei der Befragung im Rahmen der Gefährdungsbeurteilung nach § 75 Abs. 3 Nr. 11 BPersVG ab. Es sah bei der Ausfüllung der §§ 5 und 6 ArbSchG nur vorbereitende Handlungen für Maßnahmen und deshalb nur „Informations- und Anhörungsrechte" (BVerwG vom 14.10.2002, Az.: 6 P 7/01). Die Mitbestimmung nach dem BPersVG greift danach erst bei Entscheidungen über konkrete technische, organisatorische und personenbezogene Maßnahmen.

3.7 Beteiligungs- und Kontrollrechte des BR/PR

Der Interessenvertretung muss die Möglichkeit eingeräumt werden, die Einhaltung der Vereinbarung durch den Arbeitgeber effektiv und ohne dessen Einwilligung prüfen zu können (§ 80 Abs. 2 BetrVG und § 68 Abs. 2 BPersVG). Die Ausübung der Kontrolle ist allerdings in der Praxis durchaus schwierig. Riesige Protokolldateien zu überprüfen überfordert fast jeden Betriebsrat. Wahrscheinlich ist die Möglichkeit von Stichproben ein gutes Verfahren. Voraussetzung ist ein Zugang mit Berechtigung zum MDM-System.
Immer noch schwierig bleibt auch bei einem offenen System die Kontrolle, ob etwas unterlassen wurde. Wurde beispielsweise das Aufschalten auf mobile Geräte untersagt, stellt sich die Frage: Wie kann die Einhaltung kontrolliert werden? Für den Betriebsrat sehr komfortabel ist die nachstehende Regelung. Sie verpflichtet den Arbeitgeber nachzuweisen, dass Sicherheitsvorkehrungen getroffen wurden und wie diese aussehen.

> „Der BR kann jederzeit einen Nachweis darüber verlangen, welche Sicherheitsvorkehrungen hinsichtlich des Zugriffs durch unberechtigte Dritte auf die auf den mobilen Endgeräten befindlichen Daten getroffen werden."
>
> DATENVERARBEITUNG U. SOFTWAREENTWICKLUNG, 090202/210/2014

Wann ist der Betriebsrat bei Änderungen am System wieder zu beteiligen? Eine weitere Frage, die schwierig zu lösen ist. Was ist ein Update bezogen auf neue Sicherheitsanforderungen? Was ist eine Versionsänderung – ein Update mit neuen Inhalten? Keine Diskussion, ob Update oder Versionsänderung, lässt die nachstehende Regelung zu: Der Personalrat ist immer zu beteiligen.

> „Bei Änderungen bzw. Weiterentwicklung des in Anlage 1 dokumentierten Zustandes [der Firma] oder bei Einsatz zusätzlicher Komponenten oder Module ist der Konzernbetriebsrat rechtzeitig und umfassend zu informieren, um die Erforderlichkeit und Verhältnismäßigkeit prüfen und die konkrete Umsetzung beraten und mitbestimmen zu können."
>
> VERLAGS- UND DRUCKGEWERBE, 090202/209/2013

Sinnvollerweise wird der Interessenvertretung das Recht eingeräumt, sachverständige Unterstützung hinzuzuziehen. Sicher vermag nicht jede Betriebsrätin bzw. jeder Betriebsrat, ein Softwaresystem so weit zu durchdringen, dass Einstellungen auf der Admin-Ebene deutlich werden.

> „Der Betriebsrat hat das Recht, zur Wahrnehmung seiner Mitbestimmungs- und Kontrollrechte nach Rücksprache mit dem Arbeitgeber einen externen Sachverständigen hinzuzuziehen. Dies gilt insbesondere für den Fall, dass die Kontrollen und Auskunftsersuchen des Betriebsrats nicht zu einer aussagekräftigen Beurteilungsgrundlage geführt haben."
>
> LEASINGUNTERNEHMEN, 090202/196/2012

3.8 Konfliktschlichtungsverfahren

Werden sich Betriebsrat und Arbeitgeber bei Verhandlungen nicht einig, tritt das gesetzlich vorgesehene Konfliktschlichtungsverfahren in Kraft. Bei Vereinbarungen, die Gegenstände betreffen, die der vollen Mitbestimmung unterliegen, besteht das Recht, die Einigungsstelle (§ 76 BetrVG) anzurufen. Diese entscheidet im betrieblichen Bereich abschließend (§ 87 Abs. 2 BetrVG). Im Personalvertretungsrecht gilt diese Regelung grundsätzlich auch. Sie ist jedoch mit vielen Ausnahmen versehen (vgl. http://www.boeckler.de/596_22835.htm) und nur selten trifft die Einigungsstelle eine abschließende Entscheidung.
In den Vereinbarungen finden sich in Form des Einigungsstellenverfahrens verschiedene Konfliktlösungsregeln; sie betreffen Konflikte zwischen Beschäftigten und Unternehmen oder Konflikte, die aus dem unterschiedlichen Verständnis der Vereinbarung entstehen. Mit diesen Konfliktlösungsregeln wird der klagerechtliche Anspruch der einzelnen Beschäftigten nicht ausgeschlossen. Aber sie bieten die Möglichkeit, arbeitsgerichtliche Verfahren durch eine interne Schlichtung zu vermeiden.

> „Stellt der GBR begründet fest, dass mitbestimmungspflichtige Tatbestände in den Änderungen vorliegen, nehmen Bank und GBR unverzüglich Verhandlungen mit dem Ziel einer einvernehmlichen Regelung auf. Im Fall der Nichteinigung können beide Seiten die Einigungsstelle gem. § 76 Abs. 5 Betriebsverfassungsgesetz (BetrVG) anrufen. Änderungen werden nur dann vor Abschluss einer diesbezüglichen Regelung bzw. vor Beendigung des Einigungsstellenverfahrens eingeführt, wenn die Bank begründet vorträgt, dass der Bankbetrieb andernfalls gefährdet ist."
>
> KREDITGEWERBE, 090202/220/2012

Die Einigungsstelle als Streitschlichter für Auslegungsfragen der Vereinbarung ist ein Versuch, den Konflikt im Unternehmen zu schlichten. Kritisch ist die Klausel im nachstehenden Ver-

einbarungstext, wonach auch Änderungen über eine Einigungsstelle erreicht werden könnten, ohne dass die Vereinbarung gekündigt werden muss. Mit solch einer Klausel können Kompromisse im Nachhinein über Änderungswünsche aufgehoben werden. Beispiel: Eine Partei stimmt dem Verbot des Aufschaltens zu und erhält dafür bestimmte Auswertungsmöglichkeiten. Ein halbes Jahr später äußert sie den Änderungswunsch, dass nun für die Unternehmenssicherheit ein temporäres Aufschalten nötig sei (!). Müsste die Partei die Betriebsvereinbarung kündigen, würde sie sich überlegen, ob es sich lohnt. Ihre erreichten Auswertungsmöglichkeiten wären nämlich auch wieder in Gefahr.

> „Falls sich AG [Arbeitgeber] und BR nach Abschluss der Betriebsvereinbarung über gewünschte Änderungen der Betriebsvereinbarung, einschließlich ihrer Anlage nicht einigen oder im Fall eines Streits über die Auslegung oder Anwendung dieser Betriebsvereinbarung kann der AG oder der BR die Einigungsstelle anrufen. Diese Betriebsvereinbarung bleibt des ungeachtet grundsätzlich in Kraft. Unberührt hiervon bleiben Änderungen aufgrund gesetzlicher Regelungen."
>
> LEASINGUNTERNEHMEN, 090202/196/2012

In anderen Bereichen sind in den Betriebs- und Dienstvereinbarungen Schlichtungslösungen oder zumindest Schlichtungsversuche vorgesehen, laut denen eine interne Kommission mit der Aufgabe betraut wird und die Parteien so im Gespräch bleiben. Auch eine Mediation mit externer Begleitung wäre bei Konflikten gut denkbar. Unter den ausgewerteten Vereinbarungen fanden sich derartige Regelungen nicht – vielleicht weil viele in eine Rahmen-IT-Vereinbarung eingebettet waren.

4 Offene Probleme

Die MDM-Software erfordert Schutz- und Begrenzungsregelungen in den Bereichen IT-Anwendungen sowie Mobile Endgeräte bzw. Telefonie, um die Beschäftigten vor einer ständigen Überwachung und Leistungskontrolle zu schützen und ihre privaten Daten zu sichern. MDM ermöglicht es, Gespräche der Beschäftigten mit den mobilen Geräten mitzuhören, indem ein Aufschalten auf die Geräte technisch möglich ist. Über MDM können aber auch Mikrofon und Kamera der mobilen Geräte angesprochen, aktiviert und unbemerkt genutzt werden. Die Bildschirmoberflächen der mobilen Arbeitsmittel können in regelmäßigen – auch sehr kurzen – Abständen „fotografiert" werden. Diese Daten sind speicherbar, mit anderen Daten kombinierbar (z. B. GPS-Ortung) und auswertbar. Die Nutzerinnen und Nutzer der mobilen Geräte müssen also ständig damit rechnen, dass ihre Aktivitäten, ihre Gespräche und ihre Kontakte mitgehört, mitgeschnitten oder gefilmt werden. Dies stellt einen tiefen und insbesondere bei zulässiger privater Nutzung der mobilen Geräte einen unzulässigen Eingriff in die grundgesetzlich geschützten Persönlichkeitsrechte des Einzelnen dar.
Die MDM-Systeme als Verwaltungssoftware zu beschreiben und auf das Inventarisieren und Verwalten abzustellen, wird den Systemen nicht gerecht. Es geht nicht nur um den Standort der Geräte – sondern um deren Inhalte, um den Standort der Nutzerinnen und Nutzer sowie um deren beobachtbares Verhalten. In einigen ausgewerteten Vereinbarungen wird deutlich, welch tiefe Einblicke in die Verhaltensweisen der Menschen im Betrieb die neuen Arbeitsgeräte und Arbeitsformen gewähren. Dies soll eingeschränkt werden, indem man Verhaltens- und Leistungskontrollen begrenzt, den Einsatz von GPS oder das Aufschalten der Software verbietet. In vielen Vereinbarungen fehlt dieser umfassende Ansatz jedoch und ein ausreichendes Problembewusstsein scheint nicht vorhanden zu sein.
Privatheit wird transparent und wird in den Vereinbarungen durchgängig zu wenig geschützt. Private Daten, private Fotos sowie private Gespräche gehen den Arbeitgeber nichts an. Diese Informationen sind auch grundgesetzlich besonders geschützt. Für diesen Bereich wäre es erforderlich, den Zugriff durch den Arbeitgeber oder durch von ihm beauftragte Dritte tech-

nisch zu verhindern. Eine Speicherung privater Daten auf den IT-Systemen des Unternehmens sollte nur mit der ausdrücklichen Zustimmung der Betroffenen erfolgen dürfen.
Natürlich bleibt auch die Betriebsratstätigkeit mit dem mobilen Gerät nicht mehr geheim, in dem Sinne, dass Dritte keinen Zugriff haben. Regelungen zu diesem Bereich sind nicht vorhanden. Nötig wäre es wahrscheinlich, die mobilen Geräte des Betriebsrates nicht durch MDM verwalten zu lassen. Für die BR-Tätigkeit eigene Geräte zur Verfügung zu stellen oder auch hier eine technisch sichere Trennung und Verhinderung von Aufschalten und Speichern zu ermöglichen, wäre ein gangbarer Weg.
In einigen Vereinbarungen wurden Gefährdungsanalysen zur physischen und psychischen Belastung vereinbart. Dabei sollte auch die Software-Ergonomie und die Ergonomie der mobilen Geräte mit einbezogen werden. Es ist darüber hinaus notwendig, Regeln zum Schutz der Beschäftigten vor Überlastung, zum Datenschutz und als Risikomanagement zu schaffen. Denn: Die Risiken für die Beschäftigten steigen. Sie geben mit der Internetnutzung ihre persönlichen Daten preis und stehen unter Kontrolle und Druck, ständig online zu sein.
Betriebs- und Dienstvereinbarungen müssten die unterschiedlichen Seiten des MDM-Funktionsumfangs regeln sowie Persönlichkeitsschutz, Abhör- und „Abfilmschutz“, Schutz vor Leistungskontrolle, Datenschutz und Ordnungsregelungen beinhalten. Bestehen in den Unternehmen oder Dienststellen Rahmenvereinbarungen zu IT-Technik, Datenschutz oder Telefonie, so sind diese durch den „Baustein“ MDM-Software zu ergänzen und anzupassen. Bestehende Vereinbarungen zu Arbeitszeit, Gefährdungsanalysen, Telearbeit oder mobiler Arbeit sollten aktualisiert und angepasst werden.
Nur wenige Vereinbarungen enthalten erste Ansätze, um Arbeitsverdichtung zu vermeiden und Arbeitszeiten zu begrenzen. Der Schutz der Freizeit und die klare Beschreibung zulässiger Anforderungen ist ein wichtiges, bisher wenig beleuchtetes Thema. Auch die Bezahlung von Arbeitszeit außerhalb der geschuldeten Arbeitszeit, wenn beispielsweise abends noch dienstliche Mails bearbeitet werden, wird nur in wenigen Vereinbarungen angesprochen. Teils wird eine Bezahlung ausgeschlossen, teils wird nur gezahlt, was vorher genehmigt wurde. Die Selbstverständlichkeit, dass die für das Unternehmen geleistete Arbeit auch bezahlt wird, findet sich in keiner Vereinbarung. Ein weiteres Problem ist die Möglichkeit, gegen das Arbeitszeitgesetz zu verstoßen.
Tarifverträge könnten dieses Thema aufnehmen und Grundregeln aufstellen, die beispielsweise den Persönlichkeitsschutz der Beschäftigten sicherstellen. Eine tarifliche Regelung war bei den Auswertungen aber bisher nicht anzutreffen. Demgegenüber werden die Sicherheitsrisiken für die Unternehmen in den Vereinbarungen umfangreich abgebildet und Schutzregelungen getroffen sowie Verbote und Sanktionen für Missbrauch ausgesprochen. Die Unternehmensseite scheint die Probleme der IT-Sicherheit und des Datenschutzes hinsichtlich der Unternehmensdaten erkannt zu haben. Entsprechendes sollte auch für den Schutz der Beschäftigten gelten.

5 Beratungs- und Gestaltungshinweise

Aus mitbestimmungsrechtlicher Sicht ist für Betriebs- und Personalräte die Ausgangslage sehr gut, da der Einsatz von MDM-Systemen der vollen Mitbestimmung unterliegt. Volle Mitbestimmung bedeutet: Diese Software darf nicht ohne Zustimmung der Interessenvertretung oder einer Entscheidung der Einigungsstelle eingeführt werden. Die in Kapitel 3 aufgeführten Mitbestimmungsrechte zeigen die Vielfalt der angesprochenen Bereiche. Betriebs- und Dienstvereinbarungen zu diesem Thema sind daher vergleichsweise komplex gestaltet und nicht mit drei Sätzen erledigt. Die Aufgabe von MDM ist die Administration und Überwachung von mobilen Arbeitsgeräten. Daher bietet es sich in der Praxis an, die Regeln für mobile Endgeräte und MDM zumindest abzustimmen, wenn nicht sogar in einer Vereinbarung zusammenzufassen.

5.1 Gestaltungsraster

Die nachstehend zusammengefassten Gestaltungspunkte umfassen die wichtigsten Hinweise für die Gestaltung von Betriebs- und Dienstvereinbarungen bezüglich der Nutzung von MDM-Systemen und gleichzeitig von Handys, Smartphones, Blackberrys und Tablets. Die nur für MDM notwendigen und sinnvollen Inhalte sind nachfolgend kursiv dargestellt. Die Vorschläge sind nicht als fertige Vereinbarung oder Muster zu verstehen. Der Katalog muss mit eigenen Überlegungen ergänzt werden, die die jeweiligen betrieblichen Belange berücksichtigen.

- Präambel
  - *kein Aufschalten auf die mobilen Geräte (zumindest nicht ohne Einverständnis und Wissen der Beschäftigten)*
  - *keine Leistungs- und Verhaltenskontrolle – auch nicht über dritte Stellen*
  - *Gefährdungsanalyse zu physischen und psychischen Auswirkungen*
  - keine Ausweitung der Arbeitszeit/Rufbereitschaft
  - *nur einvernehmliche Änderungen/Erweiterungen der Vereinbarung*

- Geltungsbereich (beschreibt, für wen die Vereinbarung gilt)
  - Außendienst
  - Innendienst
  - Heimarbeitsplätze
  - Telearbeit
  - *Arbeit mit mobilen Geräten*

- Geräte, Begriffsbestimmungen
  - Beschreibung der genutzten Geräte, Applikationen und Dienste
    - Handy
    - Smartphone
    - Tablet
    - BYOD: Verbot oder Erlaubnis, eigene Geräte zu nutzen
    - Verkehrsdaten der Telefonie
    - *personenbezogene Daten der Beschäftigten*
    - Telefonkonferenz
    - Webkonferenz
    - *abhören, mithören, aufschalten etc.*
    - *Remote-Control*
    - *MDM-Systeme*

- Eingesetzte Software – Nutzungskonzepte und Berechtigungslisten
  - *MDM-Systeme*
  - Applikationen auf den Geräten
  - *Black-List oder White-List*
  - *Betriebskonzept*
  - *MDM-Systemhersteller, Name, Version*
  - *Regeln zum Server (Ort, eigene oder externe Geräte)*
  - *Anlage mit Systemkomponenten, Schnittstellen*
  - *Anlage mit zugelassenen Funktionen, Konfiguration und Sicherheitseinstellungen*
  - *Containerfunktion (Datensafe), Backup-Funktion*
  - *Sicherung privater Daten*
  - Cloud-Dienste

- Grundsätze
  - *Allgemein gültige Regeln*
    - *keine Leistungs- und Verhaltenskontrolle*
    - *zulässige anonyme Auswertungen*
    - *Zweckbestimmung*
    - Rufumleitung, Ortungsdienst
    - *Mithören oder Aufschalten ist unzulässig*
    - *kein Zugriff auf GPS-Daten der mobilen Geräte*
    - *kein Zugriff auf Kamera oder Mikrofon der mobilen Geräte*
    - *BOYD: private Nutzung*
    - *Gefährdungsanalyse hinsichtlich physischer und psychischer Belastungen*

- Anforderung an Ergonomie und Gesundheitsschutz
  - Arbeitsplatz-, Arbeitsumgebungs- und Gefährdungsanalyse
  - psychische Faktoren (Stressvermeidung, unbelastete Freizeit)
  - Sicherheit (PKW-Freisprecheinrichtung etc.)
  - Ergonomie der Geräte
  - *Ergonomie der Software*

- Qualifizierung
  - *Regeln etablieren*
  - *Umgang mit der Technik*
  - klare und umfassende Verhaltensregeln für Beschäftigte
  - Verhalten im Internet: Netiquette

- Arbeitszeitregelungen
  - Bereitschaftsdienste
  - *Arbeit mit mobilen Geräten = Anrechnung als Arbeitszeit*
  - Aktivierungspflicht
  - *Recht auf Abschalten, ggf. auch Pflicht bei dienstlicher Nutzung*

- Datenschutz und Datensicherung
  - *personenbezogene Daten*
  - *Unternehmensdaten*
  - *private Daten*
  - *Backup*
  - Schutzrecht Dritter
  - *Schutz vor Missbrauch und Auswertung bei externen Stellen (z. B. Cloud, MDM-Dienstleister)*

- Sanktionen
  - Schutz vor Missbrauch
  - Auswertungsregeln
  - *Schutz vor arbeitsrechtlichen Sanktionen und keine „automatische" Strafanzeige*
  - Folgen missbräuchlicher Nutzung (Arbeitgeber einerseits, Arbeitnehmer andererseits)
  - kein Schadenersatz bei Verlust von Daten, Geräten oder Einlass von Schadsoftware etc.

- Rechte der Beschäftigten
  - *Dateneinsicht: Was ist wo wie lang gespeichert?*
  - *Datenkorrektur*
  - Beschwerderecht, Überlastungsanzeigen

- Mitbestimmung und Kontrollrechte von Betriebsrat/Personalrat
  - Art und Weise der Kontrolle auch bei externen Stellen
  - *nur einvernehmliche Erweiterungen*
  - *Beteiligung bei Auswertungen*
  - *Mitbestimmung bei Qualifizierung, Gesundheitsschutz, Verhaltens- oder Ordnungsregeln, Arbeitszeit*
  - *Recht auf sachverständige Unterstützung*
  - *Einigungsverfahren im Streitfall bis zur Einigungsstelle*

- Schlussbestimmungen
  - *Laufzeit*
  - *Vereinbarung einer Probezeit für die Einführung von MDM*
  - *Nachwirkung*
  - *Kündigungsmöglichkeiten*

5.2 Ausgangspunkte für die gestaltende Einflussnahme durch die Interessenvertretung

Die ausgewerteten Vereinbarungen zeigen: Ein Problembewusstsein ist nicht bei allen Interessenvertretungen in notwendigem Umfang vorhanden. Häufig fehlt das Wissen über die Möglichkeiten der MDM-Systeme. Die Interessenvertretungen und idealerweise auch die Arbeitgeberseite sollten sich vor der Einführung informieren und beraten lassen. Daher liegt es nahe, in einem ersten Schritt sachkundige Beschäftigte oder Sachverständige heranzuziehen, die die Möglichkeiten und Risiken aufzeigen können. Es gilt das MDM-System zu verstehen und die Möglichkeiten zu durchdringen. Nur so kann eine gute Betriebs- oder Dienstvereinbarung zum Schutz der Beschäftigten entstehen.
Dies gilt auch für die Bereiche Ergonomie und Gesundheit. So ist die Bildschirmarbeitsverordnung nicht außer Kraft und gilt auch für die Arbeit mit den kleinen mobilen Geräten, Notebook oder Tablet. In Verbindung mit dem Arbeitsschutzgesetz ist eine Gefährdungsbeurteilung ein wichtiges Element, um spätere gesundheitliche Schäden der Beschäftigten zu vermeiden.
Nicht zuletzt sollte das Wissen im Bereich Datenschutz optimiert werden. Dies betrifft sowohl die Unternehmensdaten als auch die personenbezogenen Daten der Beschäftigten sowie deren private Daten. Es fallen sehr viele personenbezogene Daten an, die von MDM-Systemen verarbeitet, gespeichert und ausgewertet werden können. Hier stellen sich beispielsweise Fragen nach der datenschutzrechtlichen Zulässigkeit und den Kontrollmöglichkeiten der Interessenvertretungen.
Die Mitbestimmungsmöglichkeiten werden in Kapitel 3 beschrieben. Im Folgenden werden die wichtigsten gesetzlichen Grundlagen dargestellt. Die mitbestimmungsrechtlichen Grundlagen unterscheiden sich für Betriebs- und Personalräte teilweise erheblich. Innerhalb der Bundesländer gibt es dazu weitere Differenzierungen zu beachten. Daher wird die Rechtslage mit den Verweisen auf die jeweils geltenden Regelungen differenziert beschrieben.

5.3 Wesentliche rechtliche Grundlagen

Die wichtigsten Mitbestimmungsrechte und gesetzlichen Grundlagen werden nachstehend aufgezeigt und die Regelungen für Personalräte tabellarisch aufgeführt.

5.3.1 Verhalten und Ordnung im Betrieb

Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG setzt es nicht als notwendig voraus, dass es sich um verbindliche Verhaltensregeln handelt. Es reicht aus, wenn die Maßnahme da-

rauf gerichtet ist, das Verhalten der Arbeitnehmer zu steuern oder die Ordnung des Betriebs zu gewährleisten (BAG vom 18.04.2000, Az.: 1 ABR 22/99).
Mitbestimmungspflichtig sind gemäß § 75 Abs. 3 Ziff. 15 BPersVG Regelungen der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten.

Bayern	Art. 76 Abs. 1 Nr. 2 BayPVG (Achtung: nur Mitwirkung!)
Baden-Württemberg	§ 79 Abs.1 Nr. 12 BaWüPersVG
Berlin	§ 85 Abs. 1 Nr. 6 BlnPersVG
Brandenburg	§ 66 Ziff. 9 BraPersVG
Bremen	§ 52 BremPersVG
Hamburg	§ 86 Abs.1 Ziff. 3 HmbPersVG
Hessen	§ 74 Abs. 1 Ziff. 7 HPVG
Mecklenburg-Vorpommern	§ 70 Abs. 1 Nr. 8 PersVG MV
Niedersachsen	§ 66 Abs. 1 Nr. 10 NPersVG
Nordrhein-Westfalen	§ 72 Abs. 4 Nr. 9 LPVG NW
Rheinland-Pfalz	§ 80 Abs. 1 Nr. 11 LPersVG RP
Saarland	§ 78 Abs. 1 Nr. 14 SPersVG
Sachsen	§ 80 Abs. 3 Nr. 14 SächsPersVG
Sachsen-Anhalt	§ 65 Abs. 1 Nr. 12 PersVG LSA
Schleswig-Holstein	§ 51 MBG Schl.-H.
Thüringen	§ 74 Abs. 2 Nr. 8 ThürPersVG

5.3.2 Arbeitszeit

Mit MDM lässt sich feststellen, wer sich wann wo aufhält und was genau macht. Damit kann einerseits in Arbeitszeitbestimmungen eingegriffen werden, andererseits wird Arbeitszeit erfasst und damit bezahlbar. Die private Nutzung der beliebten Smartphones wird in der Praxis gern zugelassen, da damit die Erreichbarkeit der Beschäftigten in der Freizeit ohne Rufbereitschaft möglich ist – was ein Problem darstellen kann.
Die Mitbestimmungsrechte in § 87 Abs. 1 Nr. 2 und 3 BetrVG gewähren den Betriebsräten in diesem Bereich ein volles Mitbestimmungsrecht. Sie können initiativ tätig werden und neue Vereinbarungen verlangen. Über die vorgesehenen Einigungsstellen ist es möglich, Streitigkeiten abschließend beizulegen.
Auch die Personalräte sind hinsichtlich Verteilung, Beginn und Ende der täglichen Arbeitszeit im Rahmen der vollen Mitbestimmung zu beteiligen (§ 75 Abs. 3 Nr. 1 BPersVG). Ein eingeschränktes Mitbestimmungsrecht besteht hingegen für nicht vorhersehbare Mehrarbeit oder Überstunden gemäß § 75 Abs. 4 BPersVG.

Bayern	Art. 74 Abs. 4 Nr. und Satz 2 BayPVG
Baden-Württemberg	§ 79 Abs. 1 Nr. 1 und Satz 2 BaWüPersVG
Hessen	§ 74 Abs. 1 Nr. 9 und Abs. 2 HPVG
Saarland	§ 78 Abs. 1 Nr. 1 und Abs. 2 SPersVG
Sachsen	§ 80 Abs. 3 und Abs. 4 SächsPersVG
Sachsen-Anhalt	§ 65 Abs. 1 Nr. 1 und 2 und Abs. 2 PersVG LSA
Thüringen	§ 74 Abs. 2 Nr. 12 und Abs. 3 ThürPersVG

In Rheinland-Pfalz finden sich in § 80 Abs. 2 Nr. 5 LPersVG RP die Beteiligung zu Arbeitszeitverteilung einschließlich vorhersehbarer Mehrarbeit oder Überstunden und in § 80 Abs. 2 Nr. 4 LPersVG RP eine ausdrückliche Regelung für Bereitschaftsdienste.
Sehr ausführlich ist in § 66 Abs. 1 Nr. 1 BraPersVG die Beteiligung geregelt: „Regelungen über Beginn und Ende der täglichen Arbeitszeit und der Pausen sowie Verteilung der Arbeitszeit

auf die einzelnen Wochentage, Einführung, Ausgestaltung und Aufhebung der gleitenden Arbeitszeit und Erstellung entsprechender Pläne, Anordnung von Überstunden oder Mehrarbeit, soweit sie vorauszusehen oder nicht durch Erfordernisse des Betriebsablaufs oder der öffentlichen Sicherheit und Ordnung bedingt sind, sowie allgemeine Regelung des Ausgleichs von Mehrarbeit, Bereitschaftsdienst, Rufbereitschaft und Erstellung entsprechender Pläne."
Niedersachsen teilt die Mitbestimmung hinsichtlich Inhalt und Durchsetzungskraft auf:
§ 66 Abs. 1 Nr. 1 NPersVG – Arbeitszeit: volle Mitbestimmung
§ 66 Abs. 1 Nr. 2 NPersVG – Bereitschaft: volle Mitbestimmung
§ 67 Abs. 1 Nr. 7 NPersVG – vorhersehbare Mehrarbeit/Überstunden: nur „Mitwirkung".
In den weiteren Bundesländern finden sich umfassende Regelungen einschließlich Bereitschaft und vorhersehbarer Mehrarbeit, soweit nicht sowieso durch die Allzuständigkeit erfasst:

Berlin	§ 85 Abs. 1 Nr. 1 und 2 BlnPersVG
Bremen	§ 50 BremPersVG
Hamburg	§ 7 HmbPersVG
Mecklenburg-Vorpommern	§ 70 Abs. 1 Nr. 6 PersVG MV
Nordrhein-Westfalen	§ 72 Abs. 4 Nr. 1 und 2 LPVG NW
Schleswig-Holstein	§ 51 MBG Schl.-H.

5.3.3 Leistungs- und Verhaltenskontrolle

§ 87 Abs. 1 Nr. 6 BetrVG räumt dem Betriebsrat ein Mitbestimmungsrecht ein bei „der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen". Diese Vorschrift verlangt keine Absicht, diese Kontrollen auszuführen. Das Mitbestimmungsrecht wird bereits ausgelöst, wenn die Einrichtung dazu geeignet ist, die Kontrolle zu ermöglichen.
Die mobilen Geräte sind mittels MDM-Systeme über GPS ständig ortbar und über aufgespielte Programme jederzeit abfragbar und auswertbar. Damit ist neben den gespeicherten Daten eine weite Verhaltens- und Leistungskontrolle der Beschäftigten möglich. Die Software speichert zudem jeden Zugriff und ermöglicht direkt oder beim Anbieter der Software eine erweiterte Leistungs- und Verhaltenskontrolle.
Mit § 75 Abs. 3 Nr. 17 BPersVG gibt es eine inhaltsgleiche Regelung für Personalräte. Das Bundesverwaltungsgericht (BVerwG vom 31.8.1988, PersR 1988, 271) unterscheidet danach, ob die technische Einrichtung zur Überwachung geeignet oder bestimmt ist. Dies wird von dem Gericht immer dann unterstellt, wenn die technische Einrichtung für einen Überwachungsvorgang eingesetzt werden kann. Damit genügt auch hier die Möglichkeit.
In einigen Bundesländern genügt es dem Wortlaut nach, dass die Einrichtung „geeignet ist"; in anderen muss die Einrichtung ausdrücklich „dazu bestimmt sein", das Verhalten und die Leistung zu kontrollieren. Im Folgenden findet sich eine Übersicht über die einzelnen Paragrafen des jeweiligen LPersVG. Abweichungen zum BPersVG werden aufgeführt.

Bund	§ 75 Abs. 3 Ziff. 17 BPersVG
Bayern	Art. 75 a Abs. 1 Ziff. 1 BayPVG: Einführung, Anwendung und erhebliche Änderung technischer Einrichtungen zur Überwachung des Verhaltens oder der Leistung der Beschäftigten.
Baden-Württemberg	§ 79 Abs. 3 Nr. 12 BaWüPersVG
Berlin	§ 85 Abs.1 Nr. 13 b) BlnPersVG
Brandenburg	§ 65 Nr. 2 BraPersVG: Einführung, Anwendung, Änderung oder wesentliche Erweiterung von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.
Bremen	§ 52 BremPersVG
Hamburg	§ 87 Abs. 1 Nr. 32 HmbPersVG
Hessen	§ 74 Abs. 1 Nr. 17 HPVG: Einführung, Anwendung, wesentliche Änderung oder Erweiterung von technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.
Mecklenburg-Vorpommern	§ 70 Abs. 1 Nr. 2 PersVG MV: Einführung, Anwendung, wesentliche Änderung oder wesentliche Erweiterung von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.
Niedersachsen	§ 67 I Nr. 2 NPersVG: Einführung und Anwendung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.
Rheinland-Pfalz	§ 80 Abs. 2 Nr. 3LPersVG RP: Einführung, Anwendung, Änderung oder Erweiterung von Verfahren, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen.
Saarland	§ 84 Nr. 2 SPersVG
Sachsen	§ 80 Abs. 3 Nr.16 SächsPersVG
Sachsen-Anhalt	§ 69 Nr. 2 PersVG LSA
Schleswig-Holstein	§ 51 MBG Schl.-H.
Thüringen	§ 74 Abs. 2 Nr. 11 ThürPersVG

Einen Sonderweg geht Nordrhein-Westfalen: Es lässt eine mitbestimmungsfreie Einführung von technischen Einrichtungen zu, wenn eine Überwachung ausgeschlossen ist. § 72 Abs. 3 Nr. 2 LPVG NW: Einführung, Anwendung und Erweiterung technischer Einrichtungen, es sei denn, dass deren Eignung zur Überwachung des Verhaltens oder der Leistung der Beschäftigten ausgeschlossen ist.

5.3.4 Datenschutz

Ausgehend vom Grundrecht auf Datenschutz (Art. 2 und Art. 1 GG, vgl. Kap. 3.1) gibt es die Datenschutzgesetze im Bund und in den Bundesländern. Das BDSG ist als Verbot mit einem sogenannten Erlaubnisvorbehalt konzipiert (§ 4 BDSG). Eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist danach nur erlaubt, wenn dies durch das BDSG oder eine andere Rechtsvorschrift zugelassen wurde oder die/der Betroffene eingewilligt hat. Auch für das Beschäftigungsverhältnis gilt, dass nicht einfach alle anfallenden personenbezogenen Daten vom Unternehmen genutzt werden dürfen. Dies ist grundsätzlich nur im Rahmen des § 32 BDSG zulässig:

„§ 32 BDSG Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses
(1) 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. […].“

Soweit private Daten der Beschäftigten, ihr Aufenthaltsort, die E-Mail-Inhalte und privaten Adressen betroffen sind, handelt es sich um besonders sensible Daten im Sinne von § 3 Abs. 9 BDSG. Für diese sind nach § 4a Abs. 3, § 28 Abs. 6 bis Abs. 9 BDSG erhöhte Anforderungen an die Erhebung und Speicherung zu stellen (BAG vom 23. August 2012 – 8 AZR 804/11). Daher wird für diesen Fall auch weiterhin eine ausdrückliche Einwilligung der Beschäftigten nach § 4a BDSG erforderlich sein (Däubler et al. 2013, § 32 Rn. 10).

„§ 4a Einwilligung
(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.
(2) […].“

Der Betriebsrat ist zu beteiligen hinsichtlich der Fragen: Welche Daten der Beschäftigten dürfen überhaupt erfasst und gespeichert werden? Wie dürfen diese Daten verwendet werden? Wie dürfen sie verknüpft und ausgewertet werden? (§ 87 Abs. 1 Ziff. 6 BetrVG) Der Schutz der Persönlichkeitsrechte der Beschäftigten ist dabei das zentrale Ziel.
Eine weitere indirekte Mitbestimmungsmöglichkeit stellt § 94 BetrVG dar. Auch wenn das Unternehmen Daten der Beschäftigten selbst nicht speichert und verarbeitet, ist das Bereitstellen einer Eingabemöglichkeit von personenbezogenen Daten mitbestimmungspflichtig. Denn die Erhebung von personenbezogenen Daten der Beschäftigten ist ein Personalfragebogen im Sinne des § 94 BetrVG (BAG vom 22.10.1986, Az.: 5 AZR 660/85).
Dies gilt auch für Personalräte. Allerdings ist für sie Datenschutz in § 68 BPersVG nicht ausdrücklich als Aufgabe des Personalrats erwähnt. Aber nach § 68 Abs. 1 Ziff. 2 BPersVG hat der Personalrat darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Gesetze von der Dienststelle durchgeführt werden (vgl. Kap. 3.4). Ein direktes Mitbestimmungsrecht zum Datenschutz findet sich im BPersVG nicht.
In den Bundesländern dagegen bestehen größtenteils ausdrückliche Mitbestimmungsrechte bei der Festlegung oder Veränderung des Umfangs der Verarbeitung personenbezogener Daten der Beschäftigten. Im Folgenden findet sich eine Übersicht über die einzelnen Paragrafen des jeweiligen LPersVG.
Im Bund und in den Bundesländern als allgemeine Aufgabe:

Bund	§ 68 Abs. 1 Nr. 2 BPersVG
Bayern	Art. 69 Abs. 1 b) BayPVG
Baden-Württemberg	§ 68 Abs.1 Nr. 2 BaWüPersVG
Berlin	§ 72 Abs. 1 Nr. 2 BlnPersVG
Brandenburg	§ 58 Abs. 1 Nr. 1 BraPersVG (Ziele der Zusammenarbeit)
Bremen	§ 54 Abs. 1 b) BremPersVG
Hamburg	§ 78 Abs. 1 Nr. 3 HmbPersVG
Hessen	§ 62 Abs. 1 Nr. 2 HPVG
Mecklenburg-Vorpommern	§ 61 Nr. 2 PersVG MV
Niedersachsen	§ 59 Abs. 1 Nr. 2 NPersVG
Nordrhein-Westfalen	§ 64 Nr. 2 LPVG NW
Rheinland-Pfalz	§ 69 Abs. 1 Nr. 2 LPersVG RP
Saarland	§ 71 b) SPersVG
Sachsen	§ 73 Abs. 1 Nr.2 SächsPersVG
Sachsen-Anhalt	§ 57 Abs. 1 Nr. 2 PersVG LSA
Schleswig-Holstein	§ 51 MBG Schl.-H.
Thüringen	§ 68 Abs. 1 Nr. 2 ThürPersVG

Die oben beschriebene speziellere Mitbestimmung bei Personalfragebogen findet in den Personalvertretungsgesetzen in folgenden Paragrafen ihre Entsprechung:

Bund	§ 75 Abs. 3 Ziff. 8 BPersVG, § 76 Abs. 2 Nr. 2 für Beamte
Bayern	Art. 75 Abs. 4 Nr. 10 BayPVG
Baden-Württemberg	§ 79 Abs. 3 Nr. 4 BaWüPersVG
Berlin	§ 85 Abs.2 Nr. 5 BlnPersVG
Brandenburg	§ 65 Nr. 13 BraPersVG
Bremen	§ 52 BremPersVG
Hamburg	§ 87 Abs. 1 Nr. 23 HmbPersVG (eingeschränkte Mitbestimmung)
Hessen	§ 77 Abs. 2 Nr. 1 HPVG
Mecklenburg-Vorpommern	§ 68 Abs. 1 Nr. 18 PersVG MV (Gestaltung des Inhalts von Personalfragebogen)
Niedersachsen	§ 66 Abs. 1 Nr. 13 NPersVG
Nordrhein-Westfalen	§ 72 Abs. 4 Nr. 17 LPVG NW
Rheinland-Pfalz	§ 78 Abs. 3 Nr. 1 LPersVG RP
Saarland	§ 80 Abs. 1 a) Nr. 12 (Beamte) b) Nr. 11 SPersVG
Sachsen	§ 80 Abs. 3 Nr. 8 (§ 81 Abs. 3 Nr. 2 Beamte) SächsPersVG
Sachsen-Anhalt	Keine
Schleswig-Holstein	§ 51 MBG Schl.-H.
Thüringen	§ 75 Abs. 3 Nr. 3 ThürPersVG (eingeschränkte Mitbestimmung)

5.3.5 Qualifizierung

Die Mitbestimmung ist hinsichtlich der Qualifizierung der Beschäftigten insbesondere als Initiativrecht wahrzunehmen. Die Initiative des Betriebsrats richtet sich auf die Einführung entsprechender betrieblicher Berufsbildungsmaßnahmen nach § 97 Abs. 2 BetrVG. Das Initiativrecht richtet sich weiter auf die Ermittlung des Berufsbildungsbedarfs (§ 96 BetrVG) und damit der Bestimmung: Wer könnte welche Qualifizierung brauchen? Dazu kann der Betriebsrat Vorschläge machen zur Teilnahme an Qualifizierungsmaßnahmen für Beschäftigte oder auch Gruppen von Beschäftigten (§ 96 Abs. 1 und § 98 Abs. 3 BetrVG).
Die Beteiligungsrechte für Betriebsräte umfassen einerseits die Inhalte von notwendigen Qualifizierungen und andererseits die Auswahl der Teilnehmerinnen und Teilnehmer. In den Personalvertretungsgesetzen finden wir keine einheitliche Beteiligungsart. Häufig ist nur eine

eingeschränkte Mitbestimmung bei der Durchführung und inhaltlichen Gestaltung gegeben und dann noch nach Angestellten und Beamten unterschieden. Bei der Auswahl ist teils die Mitbestimmung nur vorgesehen, wenn mehr Bewerberinnen und Bewerber als Plätze vorhanden sind.
Im Bund und in den Bundesländern (Abweichungen zum BPersVG werden skizziert):

Bund	§ 76 Abs. 2 Nr. 6 BPersVG (Durchführung), § 75 Abs. 3 Nr. 7 BPersVG: Auswahl der Teilnehmer an Fortbildungsveranstaltungen für Arbeitnehmer (§ 76 Abs. 2 Nr. 2 BPersVG für Beamte)
Bayern	Art. 76 Abs. 1 Nr. 7 BayPVG (Mitwirkung), Art. 76 Abs. 1 Nr. 8 BayPVG Aufstellung von Grundsätzen für die Auswahl von Teilnehmern an Fortbildungsveranstaltungen (Mitwirkung)
Baden-Württemberg	§ 79 Abs. 3 Nr. 11 BaWüPersVG, § 80 Abs. 1 Nr. 9 BaWüPersVG Auswahl der Teilnehmer an Maßnahmen der Berufsausbildung und an Fortbildungs- sowie Weiterbildungsveranstaltungen
Berlin	§ 85 Abs. 2 Nr. 1 BlnPersVG (§ 85 Abs. 1 Nr. 5 und Abs. 2 Nr. 3 BlnPersVG: Durchführung)
Brandenburg	§ 65 Nr. 12 BraPersVG
Bremen	§ 63 Abs. 1 i) BremPersVG, § 52 BremPersVG (Allzuständigkeit)
Hamburg	§ 87 Abs. 1 Nr. 18 HmbPersVG (eingeschränkte Mitbestimmung hinsichtlich Durchführung), § 87 Abs. 1 Nr. 19 HmbPersVG (eingeschränkte Mitbestimmung hinsichtlich Auswahl)
Hessen	§ 74 Abs. 1 Nr. 8 HPVG (allgemeine Grundsätze der Fortbildung)
Mecklenburg-Vorpommern	§ 68 Abs. 1 Nr. 17 PersVG MV
Niedersachsen	§ 65 Abs 1 Nr. 18 (Beamte) Abs. 2 Nr. 14 NPersVG (Aufstellung von Grundsätzen über die Durchführung der Fortbildung), § 65 Abs. 1 Nr. 19 (Beamte) Abs. 2 Nr. 13 NPersVG (Auswahl, wenn mehr Bewerber vorhanden als Plätze zur Verfügung stehen)
Nordrhein-Westfalen	§ 72 Abs. 4 Nr. 16 LPVG NW (allgemeine Fragen der Fortbildung der Beschäftigten), § 72 Abs. 4 Nr. 16 LPVG NW (Auswahl)
Rheinland-Pfalz	§ 78 Abs. 2 Nr. 16 (Auswahl), Abs. 3 Nr. 3 (Durchführung) LPersVG RP, § 79 Abs. 2 Nr. 17 u. Abs. 3 Nr. 3 LPersVG RP (Beamte), § 78 Abs. 2 Ziff. 16 LPersVG RP: Auswahl für die Teilnahme an Maßnahmen der Berufsausbildung, der beruflichen Fortbildung und der beruflichen Umschulung, wenn mehr Bewerberinnen und Bewerber vorhanden sind, als Plätze zur Verfügung stehen (bei Beamten § 79 Abs.2 Ziff. 16)
Saarland	§ 78 Abs. 1 Nr. 6 SPersVG (Durchführung),
Sachsen	§ 81 Abs. 3 Nr. 6 SächsPersVG, § 80 Abs. 3 Nr. 7 § 81 Abs. 3 Nr. 1 (Beamte) SächsPersVG (Auswahl)
Sachsen-Anhalt	§ 65 Abs. 1 Nr. 4 PersVG LSA (Durchführung)
Schleswig-Holstein	§ 51 MBG Schl.-H. (Allzuständigkeit)
Thüringen	§ 75 Abs. 3 Nr. 13 ThürPersVG (eingeschränkte Mitbestimmung), § 75 Abs. 3 Nr. 2 ThürPersVG (eingeschränkte Mitbestimmung Teilnehmerauswahl)

5.3.6 Gesundheitsschutz/Ergonomie

Gesundheit umfasst die körperliche und psychische Unversehrtheit. Gefährdungen durch die Geräte selbst, ergonomische Mindestanforderungen an die Geräte und die Software und Sicherheitsansprüche sind gemäß § 87 Abs. 1 Nr. 7 und § 91 BetrVG mitbestimmungspflichtige Themen. Regelungen wären ebenfalls sinnvoll hinsichtlich möglicher psychischer Belastungen sowie hinsichtlich der Ausdehnung von beruflichen Belangen in die Freizeit durch ständige Erreichbarkeit oder die Sichtbarkeit von beruflichen Anforderungen (zum Beispiel E-Mails) und deren belastenden Folgen wie etwa psychische oder psychosomatische Erkrankungen.

Daneben bestehen Aufklärungspflichten des Arbeitgebers gemäß § 81 Abs. 1 BetrVG und die Verpflichtung zu Schutzmaßnahmen nach den §§ 9, 10 und 12 ArbSchG. Dazu gehören auch entsprechende Gefährdungsanalysen. Die konkreten arbeitsplatz- oder aufgabenbezogenen Unterweisungen sind an den Erkenntnissen der Gefährdungsanalyse im Sinne von § 5 ArbSchG auszurichten.
Dem Betriebsrat steht ein Mitbestimmungsrecht zur Ausfüllung der Regelungen über den Gesundheitsschutz im Rahmen der gesetzlichen Vorschriften zu. Solche ausfüllungsbedürftigen Rahmenvorschriften sind beispielsweise die §§ 3 ff. ArbSchG. So besteht nach der Generalklausel des § 3 Abs. 1 ArbSchG unter anderem die Pflicht des Arbeitgebers, auf die Gesundheit der Beschäftigten zu achten und Verbesserungen des Gesundheitsschutzes anzustreben. Dabei hat er sich nach § 4 Nr. 1 ArbSchG davon leiten zu lassen, dass Gefährdungen der Gesundheit möglichst vermieden bzw. kleingehalten werden.

§ 3 ArbSchG – Grundpflichten des Arbeitgebers
(1) Der Arbeitgeber ist verpflichtet, die erforderlichen Maßnahmen des Arbeitsschutzes unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen. Er hat die Maßnahmen auf ihre Wirksamkeit zu überprüfen und erforderlichenfalls sich ändernden Gegebenheiten anzupassen. Dabei hat er eine Verbesserung von Sicherheit und Gesundheitsschutz der Beschäftigten anzustreben.
(2) Zur Planung und Durchführung der Maßnahmen nach Absatz 1 hat der Arbeitgeber unter Berücksichtigung der Art der Tätigkeiten und der Zahl der Beschäftigten
1. für eine geeignete Organisation zu sorgen und die erforderlichen Mittel bereitzustellen sowie
2. Vorkehrungen zu treffen, dass die Maßnahmen erforderlichenfalls bei allen Tätigkeiten und eingebunden in die betrieblichen Führungsstrukturen beachtet werden und die Beschäftigten ihren Mitwirkungspflichten nachkommen können.

(3) Kosten für Maßnahmen nach diesem Gesetz darf der Arbeitgeber nicht den Beschäftigten auferlegen.

§ 4 ArbSchG – Allgemeine Grundsätze
Der Arbeitgeber hat bei Maßnahmen des Arbeitsschutzes von folgenden allgemeinen Grundsätzen auszugehen:
1. Die Arbeit ist so zu gestalten, dass eine Gefährdung für Leben und Gesundheit möglichst vermieden und die verbleibende Gefährdung möglichst gering gehalten wird;
2. Gefahren sind an ihrer Quelle zu bekämpfen;
3. bei den Maßnahmen sind der Stand von Technik, Arbeitsmedizin und Hygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse zu berücksichtigen;
4. Maßnahmen sind mit dem Ziel zu planen, Technik, Arbeitsorganisation, sonstige Arbeitsbedingungen, soziale Beziehungen und Einfluss der Umwelt auf den Arbeitsplatz sachgerecht zu verknüpfen;
5. individuelle Schutzmaßnahmen sind nachrangig zu anderen Maßnahmen;
6. spezielle Gefahren für besonders schutzbedürftige Beschäftigtengruppen sind zu berücksichtigen;
7. den Beschäftigten sind geeignete Anweisungen zu erteilen;
8. mittelbar oder unmittelbar geschlechtsspezifisch wirkende Regelungen sind nur zulässig, wenn dies aus biologischen Gründen zwingend geboten ist.

§ 5 ArbSchG – Beurteilung der Arbeitsbedingungen
(1) Der Arbeitgeber hat durch eine Beurteilung der für die Beschäftigten mit ihrer Arbeit verbundenen Gefährdung zu ermitteln, welche Maßnahmen des Arbeitsschutzes erforderlich sind.
(2) Der Arbeitgeber hat die Beurteilung je nach Art der Tätigkeiten vorzunehmen. Bei gleichartigen Arbeitsbedingungen ist die Beurteilung eines Arbeitsplatzes oder einer Tätigkeit ausreichend.
(3) Eine Gefährdung kann sich insbesondere ergeben durch

1. die Gestaltung und die Einrichtung der Arbeitsstätte und des Arbeitsplatzes,
2. physikalische, chemische und biologische Einwirkungen,
3. die Gestaltung, die Auswahl und den Einsatz von Arbeitsmitteln, insbesondere von Arbeitsstoffen, Maschinen, Geräten und Anlagen sowie den Umgang damit,
4. die Gestaltung von Arbeits- und Fertigungsverfahren, Arbeitsabläufen und Arbeitszeit und deren Zusammenwirken,
5. unzureichende Qualifikation und Unterweisung der Beschäftigten.

§ 9 ArbSchG – Besondere Gefahren
(1) Der Arbeitgeber hat Maßnahmen zu treffen, damit nur Beschäftigte Zugang zu besonders gefährlichen Arbeitsbereichen haben, die zuvor geeignete Anweisungen erhalten haben. […]

§ 12 ArbSchG – Unterweisung
(1) Der Arbeitgeber hat die Beschäftigten über Sicherheit und Gesundheitsschutz bei der Arbeit während ihrer Arbeitszeit ausreichend und angemessen zu unterweisen. Die Unterweisung umfasst Anweisungen und Erläuterungen, die eigens auf den Arbeitsplatz oder den Aufgabenbereich der Beschäftigten ausgerichtet sind. Die Unterweisung muss bei der Einstellung, bei Veränderungen im Aufgabenbereich, der Einführung neuer Arbeitsmittel oder einer neuen Technologie vor Aufnahme der Tätigkeit der Beschäftigten erfolgen. Die Unterweisung muss an die Gefährdungsentwicklung angepasst sein und erforderlichenfalls regelmäßig wiederholt werden. […]

Allgemein gilt: Der Betriebsrat hat nach § 87 Abs. 1 Nr. 7 BetrVG bei betrieblichen Regelungen über den Gesundheitsschutz mitzubestimmen. Hierzu gehört auch die durch § 12 ArbSchG dem Arbeitgeber auferlegte Verpflichtung, die Beschäftigten über Sicherheit und Gesundheitsschutz bei der Arbeit zu unterweisen. Einigen sich die Betriebsparteien nicht über Art und Inhalt der Unterweisung, ist gemäß §§ 87 Abs. 2 und 76 BetrVG eine Einigungsstelle zu bilden, um den Streit beizulegen.
Für Personalräte ist in diesem Bereich jedoch die Rechtslage anders. Das höchste deutsche Verwaltungsgericht (BVerwG) lehnte im Jahr 2002 die Mitbestimmung eines Personalrats bei der Befragung im Rahmen der Gefährdungsbeurteilung nach § 75 Abs. 3 Nr. 11 BPersVG ab. Es sah bei der Ausfüllung der §§ 5 und 6 ArbSchG nur vorbereitende Handlungen für Maßnahmen und deshalb nur „Informations- und Anhörungsrechte“. Die Mitbestimmung nach dem BPersVG greift danach erst bei Entscheidungen über konkrete technische, organisatorische und personenbezogene Maßnahmen.
Wie auf Bundesebene in § 75 Abs. 3 Ziff. 11 BPersVG besteht bei Maßnahmen zur Verhütung von Dienst- und Arbeitsunfällen und sonstigen Gesundheitsschädigungen ein volles Mitbestimmungsrecht.

Übersicht im Bund und in den Bundesländern:

Bund	§ 75 Abs. 3 Ziff. 11 BPersVG
Bayern	Art. 75 Abs. 4 Ziff. 8 BayPVG
Baden-Württemberg	§ 79 Abs. 1 Nr. 8 BaWüPersVG
Berlin	§ 85 Abs.1 Nr. 7 BlnPersVG
Brandenburg	§ 66 Nr. 7 BraPersVG
Bremen	§ 63 Abs. 1 d) BremPersVG
Hamburg	§ 86 Abs. 1 Nr. 15 HmbPersVG
Hessen	§ 74 Abs. 1 Nr. 6 HPVG
Mecklenburg-Vorpommern	§ 69 Nr. 7 PersVG MV
Niedersachsen	§ 66 I Nr. 11 NPersVG
Nordrhein-Westfalen	§ 72 Abs. 4 Nr. 7 LPVG NW
Rheinland-Pfalz	§ 80 Abs. 2 Nr. 7 LPersVG RP
Saarland	§ 78 Abs. 1 Nr. 8 SPersVG
Sachsen	§ 80 Abs. 3 Nr.11 SächsPersVG
Sachsen-Anhalt	§ 65 Abs. 1 Nr. 13 PersVG LSA
Schleswig-Holstein	§ 51 MBG Schl.-H.
Thüringen	§ 74 Abs. 2 Nr. 5 ThürPersVG

6 Bestand der Vereinbarungen

Tabelle 1: Art und Anzahl der Vereinbarungen

Art der Vereinbarung	**Anzahl**
Betriebsvereinbarung	15
Dienstvereinbarung	5
Richtlinie	1
Gesamt	**21**

Tabelle 2: Verteilung der Vereinbarungen nach Branchen

Branche	**Anzahl**
Bergbau	1
Bildungseinrichtung	1
Chemische Industrie	2
Datenverarbeitung u. Softwareentwicklung	1
Energiedienstleister	1
Fahrzeughersteller Kraftwagen	2
Gesundheit und Soziales	2
Grundstücks- und Wohnungswesen	1
Kreditgewerbe	1
Landverkehr	1
Leasingunternehmen	1
Nachrichtentechnik/Unterhaltungs-, Automobilelektronik	1
Öffentliche Verwaltung	3
Papiergewerbe	1
Verlags- und Druckgewerbe	1
Versicherungsgewerbe	1
Gesamt	**21**

Tabelle 3: Abschlussjahr bzw. Änderungsjahr der Vereinbarungen

Abschlussjahr	**Anzahl**
2014	12
2013	2
2012	5
2011	0
2010	2
Gesamt	**21**

Glossar

Application (App)
Software/Programm, insbesondere Anwendungsprogramme für mobile Geräte

Bring your own device (BYOD)
Pflicht oder Möglichkeit, in der Arbeit private Kommunikationsgeräte zu nutzen.

Compliance
Regeltreue oder Regelkonformität bezogen auf die Gesamtheit der Grundsätze und Regeln eines Unternehmens.

Devices
Mobile Geräte

Global Positioning System (GPS)
Weltweites Ortungssystem

Apple iOS
Betriebssystem von Apple für die mobilen Kommunikationsgeräte iPhone, iPod touch, iPad etc.

Jailbreak
Dt. Gefängnisausbruch; Bruch von Schutzmechanismen im mobilen Kommunikationsgerät.

Mobile Device Management (MDM)
Softwaresystem zur zentralen Verwaltung, Steuerung, Auswertung und Inventarisierung von mobilen Endgeräten.

Provisioning Certificate
Zertifikatsbereitstellung auf dem mobilen Kommunikationsgerät.

Tablet/Tablet-PC
Tragbarer, flacher Computer mit berührungsempfindlichem Bildschirm.

Remote-Control/Remote-Zugriff
Zugriff auf ein entferntes System, Fernsteuerung von mobilen Geräten.

Remote-Support
Fernwartung von mobilen Geräten.

Smartphone
Mobiltelefon, das über Computerfunktionalität und Internetzugang verfügt. Über weitere Programme bzw. → Apps können das Gerät vom Anwender individuell mit neuen Funktionen ausgestattet werden.

Literaturhinweise

Baunack, Sebastian (2014): Mobile Arbeitsmittel, in: Computer und Arbeit (CuA) 2/2014, S. 8 ff.
Dahlbeck, Detlef/Sobisch, Jens (2013): Dauerüberwachung ist Stress für die Seele!, in: CuA 3/2013, S. 19 ff.
Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (2013): Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG, 4. Auflage, Frankfurt am Main.
Klein, Konrad-Jochen (2013): Mobile Sicherheit, in: CuA 9/2013, S. 7 ff.
von Lüpke, Marc (2013): Immer und überall, in: Mitbestimmung 12/2013, S. 34 ff.
Nies, Gerd/Vogl, Gerlinde (2013): Mobile Arbeit, in: CuA 9/2013, S. 10 ff.
Plath, Kai-Uwe (2012): BDSG, Kommentar, Köln.
Rozeck, Heike (2014): Zugriff des Arbeitgebers auf Kommunikationsdaten, in: CuA 9/2014, S. 30 ff.
Ruchhöft, Mattias (2012): Muss noch kurz die Welt retten, in: CuA 5/2012, S. 5 ff.
Schwemme, Michael/Wedde, Peter (2012): Digitale Arbeit in Deutschland, Potenziale und Problemlagen, Friedrich-Ebert-Stiftung (Hg.), Download unter http://library.fes.de/pdf-files/akademie/09324.pdf.
Steinwender, Frank (2013): Flöhe hüten 2.0 – Mobile Geräte im Sinne der Beschäftigten hüten, in: CuA 9/2013, S. 4 ff.
Thannheiser, Achim (2014): Mobile Kommunikation: in: CuA 2/2014, S. 5 ff.
Thannheiser, Achim (2015): Alles ist möglich – MDM-Software, in: AiB 5/2015

Das Archiv Betriebliche Vereinbarungen der Hans-Böckler-Stiftung

Die Hans-Böckler-Stiftung verfügt über die bundesweit einzige bedeutsame Sammlung betrieblicher Vereinbarungen, die zwischen Unternehmensleitungen und Belegschaftsvertretungen abgeschlossen werden. Derzeit enthält unser Archiv etwa 16.000 Vereinbarungen zu ausgewählten betrieblichen Gestaltungsfeldern.

Unsere breite Materialgrundlage erlaubt Analysen zu betrieblichen Gestaltungspolitiken und ermöglicht Aussagen zu Trendentwicklungen der Arbeitsbeziehungen in deutschen Betrieben. Regelmäßig werten wir betriebliche Vereinbarungen in einzelnen Gebieten aus. Leitende Fragen dieser Analysen sind: Wie haben die Akteure die wichtigsten Aspekte geregelt? Welche Anregungen geben die Vereinbarungen für die Praxis? Wie ändern sich Prozeduren und Instrumente der Mitbestimmung? Existieren ungelöste Probleme und offene Fragen? Die Analysen betrieblicher Vereinbarungen zeigen, welche Regelungsweisen und -verfahren in Betrieben bestehen. Die Auswertungen verfolgen dabei nicht das Ziel, Vereinbarungen zu bewerten, denn die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen und Gestaltungshinweise zu geben.

Bei Auswertungen und Zitaten aus Vereinbarungen wird streng auf Anonymität geachtet. Die Kodierung am Ende eines Zitats bezeichnet den Standort der Vereinbarung in unserem Archiv und das Jahr des Abschlusses. Zum Text der Vereinbarungen haben nur Mitarbeiterinnen und Mitarbeiter des Archivs und Autorinnen und Autoren Zugang.

Zusätzlich zu diesen Auswertungen werden vielfältige anonymisierte Auszüge aus den Vereinbarungen in einer Online-Datenbank im Internetauftritt der Hans-Böckler-Stiftung zusammengestellt. Damit bieten wir anschauliche Einblicke in die Regelungspraxis, um eigene Vorgehensweisen und Formulierungen anzuregen. Darüber hinaus gehen wir in betrieblichen Fallstudien gezielt Fragen nach, wie die abgeschlossenen Vereinbarungen umgesetzt werden und wie die getroffenen Regelungen in der Praxis wirken.

Das Internetangebot des Archivs Betriebliche Vereinbarungen ist unmittelbar zu erreichen unter www.boeckler.de/betriebsvereinbarungen.

Anfragen und Rückmeldungen richten Sie bitte an betriebsvereinbarung@boeckler.de oder direkt an

Dr. Manuela Maschke
0211-7778-224, E-Mail: Manuela-Maschke@boeckler.de
Angela Siebertz
0211-7778-288, E-Mail: Angela-Siebertz@boeckler.de
Nils Werner
0211-7778-167, E-Mail: Nils-Werner@boeckler.de