genden Sicherheitsvorgaben einhalten und für alle die Sicherheitsmaßnahmen, die nicht zentral umgesetzt werden können, Sorge tragen. Hierzu sollte das Personal über die Gefahren im Umgang mit mobilen Geräten fachkundig geschult werden.

Ferner sollten zumindest folgende Vorgaben in einer Richtlinie oder Betriebsvereinbarung verfasst werden:

- Jedes Gerät ist durch Passwörter und PINs gegen den Zugriff Dritter zu sichern. Die Weitergabe von Passwörten und PINs an Dritte ist strengstens untersagt. Der Mitarbeiter hat Sorge dafür zu tragen, dass die Passwörter und PINs auch nicht von Dritten ausgespäht werden (insbes. bei der Eingabe). Für die Erstellung der Passwörter müssen Regeln aufgestellt werden, die diese möglichst sicher gestalten (Anzahl und Art der Zeichen, begrenzte Geltungsdauer etc.).
- Bildschirmschoner oder ähnliche Zugriffssperren, die sich nach kurzer Zeit (max. fünf Minuten) automatisch einschalten und nur durch eine erneute Eingabe eines Passwortes wieder aufheben lassen, müssen aktiviert bleiben.
- Das mobile Gerät muss beaufsichtigt oder sicher gelagert werden, sodass die Gefahr eines Verlusts oder Diebstahls möglichst gering gehalten wird. Ein Ausleihen des Geräts an Dritte ist nicht gestattet. Sollte das Gerät dennoch in die Hände Dritter geraten, so ist es danach auf etwaige Abweichungen vom Regelzustand hin zu überprüfen. Im Zweifelsfall muss eine Überprüfung durch den Systemadministrator erfolgen. Jeder Verlust ist dem Systemadminstrator umgehend zu melden, damit durch diesen eine Lokalisierung bzw. ein Remote-Wipe erfolgen kann.
- Sämtliche Wartungs- und Reparaturmaßnahmen dürfen ausschließlich vom Systemadministrator oder auf dessen Weisung hin vorgenommen werden (so z. B. auch die laufende Aktualisierung des Betriebssystems). Sollte trotzdem eine Weitergabe an Dritte erfolgen (z. B. im Garantiefall an den Hersteller), so hat zuvor eine vollständige Datensicherung und ein Zurücksetzen des Gerätes auf die Grundeinstellungen (Factory-Reset) zu erfolgen.
- Eine direkte Kopplung mit anderen Geräten über WLAN, Bluetooth etc. setzt voraus, dass der Inhaber des anderen Geräts dem Mitarbeiter persönlich bekannt und vertrauenswürdig ist. Soweit derartige Dienste nicht genutzt werden, sind sie auf dem Gerät zu deaktivieren.
- Es dürfen nur Anwendungen (Programme, Apps) installiert werden, die vom Systemadministrator freigegeben sind. Eine entsprechende Liste wird ständig aktualisiert. Soweit vom Hersteller des Geräts Sperren eingerichtet sind, dürfen diese (durch ein sog. Jailbreaking) nicht umgangen werden.

Hinzu kommen noch solche Regelungen, die sich allgemein aus der dienstlichen Nutzung eines betrieblichen Kommunikationsmittels ergeben (s. o. 2.).

III. Private Nutzung betrieblicher Kommunikationsmittel

1. Begriff

Immer dann, wenn die Nutzung der betrieblichen Kommunikationsmittel nicht dienstlich veranlasst ist, liegt eine private Nutzung vor. Der Arbeitgeber kann grundsätzlich frei darüber entscheiden, ob und ggf. in welchem Rahmen er seinen Mitarbeitern eine private Nutzung gestatten will. Für die private Nutzung ist also die Genehmigung des Arbeitgebers erforderlich.

WICHTIG!

Die Weisungsbefugnis des Arbeitgebers besteht nur hinsichtlich der privaten Nutzung betrieblicher – also der vom Arbeitgeber zur Verfügung gestellten Kommunikationsgeräte und -dienste. Die private Nutzung eigener Geräte des Arbeitnehmers im Betrieb (wie z. B. Smartphone) kann nicht einschränkungslos untersagt werden. Hier muss in jedem Fall eine Interessenabwägung getroffen werden. So kann das Mitbringen von Smartphones (mit audio-visuellen Aufzeichnungsmöglichkeiten) in sicherheitsempfindliche Bereiche (z. B. in Entwicklungsabteilungen) gänzlich untersagt werden, wenn dies zur Sicherung von Betriebsgeheimnissen erforderlich ist. Einem generellen Verbot zur privaten Handynutzung, das auch die Pausen umfasst, liegen regelmäßig keine ausreichenden Arbeitgeberinteressen zu Grunde. Da es sich bei dem Verbot der Nutzung eigener Geräte im Betrieb um eine Angelegenheit der betrieblichen Ordnung handelt, besteht diesbezüglich ein Mitbestimmungsrecht des Betriebsrates.

Die Genehmigung zur privaten Nutzung betrieblicher Kommunikationsmittel kann allgemein, z. B. im Wege einer Betriebsvereinbarung, erteilt oder mit jedem Arbeitnehmer einzeln vereinbart werden. Sie kann aber auch durch eine Richtlinie oder stillschweigend gestattet werden.

ACHTUNG!

Ein Anspruch auf die Gestattung der privaten Nutzung kann sich auch aus einer betrieblichen Übung ergeben, z. B. wenn die private Nutzung über einen längeren Zeitraum hinweg vom Arbeitgeber gebilligt wird. Ist erst einmal eine betriebliche Übung entstanden, so kann der Arbeitgeber diese nicht einfach wieder beseitigen. Hierzu bedarf es der Zustimmung der Mitarbeiter oder einer Änderungskündigung. Eine ablösende Betriebsvereinbarung, mit der die private Nutzung betrieblicher Kommunikationsmittel einfach untersagt wird, kommt dann nicht (mehr) in Betracht. Mehr zum Thema: s. → *Betriebliche Übung*.

Die Gestattung der privaten Nutzung der betrieblichen Kommunikationsmittel bringt erhebliche datenschutzrechtliche Konsequenzen mit sich, da – zumindest nach Auffassung der Datenschutzaufsichtsbehörden – der Arbeitgeber insoweit als Anbieter von Telemedien und Telekommunikationsdienstleistungen i. S. d. gesetzlichen Bestimmungen (TKG, TMG) einzustufen ist. Vor einer Gestattung der privaten Nutzung sollte sich der Arbeitgeber also genau überlegen, ob er die hiermit einhergehenden Auflagen erfüllen will und kann (s. hierzu mehr unter IV. Datenschutz und Fernmeldegeheimnis).

WICHTIG!

Eine Vielzahl von Arbeitsgerichten (vgl. LAG Berlin-Brandenburg v. 14.1.2016, Az. 5 Sa 657/15 und v. 16.2.2016, Az. 4 Sa 2132/10) teilt die Auffassung der Datenschutzaufsichtsbehörden nicht und gelangt zu dem Ergebnis, dass der Arbeitgeber keine geschäftsmäßigen Telekommunikationsleistungen erbringt und somit kein Diensteanbieter i. S. d. § 3 Nr. 6 TKG sei. Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten eines Beschäftigten sei daher im Rahmen des § 32 BDSG (seit 25.5.2018 ersetzt durch § 26 BDSG) auch ohne dessen Einwilligung zulässig (LAG Berlin-Brandenburg v. 14.1.2016, Az. 5 Sa 657/15). Hieran dürfte sich auch nach der Einführung der DSGVO nichts geändert haben, wobei selbstverständlich die Rahmenbedingungen (Zweckbindung, Datensparsamkeit etc.) zu beachten sind.

2. Regelungsmöglichkeiten

Wenn der Arbeitgeber die private Nutzung betrieblicher Kommunikationsmittel gestatten will, sollte er die Rahmenbedingungen auf jeden Fall so genau wie möglich regeln.

Zunächst sollte der Umfang der erlaubten privaten Nutzung exakt bestimmt werden. Allein der Hinweis auf eine „Angemessenheit" der erlaubten Nutzung reicht i. d. R. nicht aus, um hieraus Ansprüche gegen einen Mitarbeiter herzuleiten. Vielmehr sollten klare Grenzen gesetzt werden. So kann z. B. die private Nutzung betrieblicher Kommunikationsmittel während der Arbeitszeit generell verboten bzw. die Erlaubnis auf die private Nutzung in Arbeitspausen beschränkt werden. Auch können zeitliche Grenzen für die Dauer der privaten Nutzung vor-

gegeben werden. Das Führen von Auslandstelefonaten oder die Inanspruchnahme von kostenpflichtigen Angeboten sollte zu privaten Zwecken generell verboten werden.

Für die private Nutzung von E-Mails, Messaging-Diensten oder SMS sind neben den allgemeinen Vorgaben (zur dienstlichen Nutzung) besondere Vorschriften zu erlassen.

Der Arbeitgeber ist gesetzlich dazu verpflichtet, Handelsbriefe (gem. § 238 Abs. 2 HGB) und sonstige Korrespondenz mit steuerlichem Bezug (§ 147 AO) zu archivieren. Hierzu gehören u. U. auch E-Mails und sonstige Textnachrichten (nebst Anlagen). Andererseits darf der Arbeitgeber aber auf private E-Mails und Textnachrichten des Arbeitnehmers nicht ohne weiteres zugreifen oder diese speichern. Deshalb muss der Arbeitgeber entweder aufwendige technische Lösungen betreiben, die in der Lage sind, die privaten Nachrichten von den dienstlichen zu trennen. Oder er macht die Privatnutzung ausdrücklich davon abhängig, dass die Arbeitnehmer den Zugriff auf und die Archivierung von privaten Nachrichten schriftlich gestatten.

Verboten werden sollte auf jeden Fall die private Übersendung betriebsinterner (nicht nur vertraulicher) und personenbezogener Daten sowie der Versand von Nachrichten, die einen anstößigen oder strafbaren Inhalt haben (z. B. ausländerfeindliche Parolen) oder die in irgendeiner Weise das Ansehen des Arbeitgebers schädigen könnten.

Aus Sicherheits- und Kostengründen empfiehlt es sich im Zusammenhang mit der Nutzung von Computer und Internet,

- das Herunterladen von Dateien und Programmen zur privaten Nutzung,
- das Installieren privater oder fremder Software,
- den Aufruf kostenpflichtiger Websites und
- den Besuch von Internetseiten mit anstößigem oder strafbarem Inhalt (egal, ob kostenpflichtig oder nicht)

generell zu verbieten.

TIPP!

Der Arbeitgeber sollte die Erlaubnis zur privaten Nutzung betrieblicher Kommunikationsmittel davon abhängig machen, dass sich der Arbeitnehmer mit einem vom Arbeitgeber eingeführten Kontrollsystem sowie der Archivierung und dem Zugriff auf private E-Mails schriftlich einverstanden erklärt.

3. Mobile Geräte

Unter Berücksichtigung der besonderen Risiken, die sich bereits aus der betrieblichen Nutzung mobiler Geräte ergeben (s. II.3.), birgt die Gestattung der privaten Nutzung eines solchen Geräts noch weitere Gefahren und macht zusätzliche Regelungen erforderlich. Der Arbeitgeber ist nämlich – als Verantwortlicher gem. Art. 4 Nr. 7, 24 ff. DSGVO – schon aus datenschutzrechtlichen Gründen dazu verpflichtet, die Verarbeitung von personenbezogenen Daten umfassend zu kontrollieren. Andererseits müssen aus persönlichkeitsrechtlichen Gründen private Daten des Arbeitnehmers von einer solchen Kontrolle grundsätzlich ausgenommen bleiben. Wird dem Arbeitnehmer also gestattet, ein mobiles Gerät auch privat zu nutzen, so stellt sich jeder Zugriff auf dieses Gerät seitens des Arbeitgebers potenziell auch als Eingriff in die Privatsphäre des Arbeitnehmers dar. Hierdurch werden die Kontrollmöglichkeiten erheblich eingeschränkt.

ACHTUNG!

Zwingende Voraussetzung für die Gestattung der privaten Nutzung mobiler Geräte ist daher, dass auf dem Gerät eine strikte Trennung von privaten und betrieblichen Daten erfolgt.

Die Kontrolle betrieblicher Anwendungen und Daten sollte im Rahmen eines Mobil-Device-Managements (MDM) bereits so weitreichend sein, dass neben den ohnehin erforderlichen Sicherheitsvorgaben (s. o. II.2. f.) in erster Linie nur noch die Besonderheiten der privaten Nutzung zu regeln sind. Hierzu gehören:

- die Einwilligung des Arbeitnehmers, dass die nach den datenschutzrechtlichen Bestimmungen erforderlichen Kontrollen jederzeit und einschränkungslos durchgeführt werden können;
- die Verpflichtung des Arbeitnehmers, dass eine strikte Trennung von privaten und betrieblichen Daten, Anwendungen und Benutzeraccounts erfolgt;
- die Einwilligung des Arbeitnehmers, dass bei Verlust des Gerätes auch eine Ortung (Theft-Recovery) und Sperrung sowie ggfs. eine Fernlöschung sämtlicher Daten (Remote-Wipe) erfolgt;
- Gebot, dass der Arbeitnehmer selbst für die Sicherung seiner privaten Daten Sorge zu tragen hat, bei der jedoch keine gleichzeitige Sicherung der betrieblichen Daten auf anderen als den vom Arbeitgeber vorgegebenen Datenträgern erfolgen darf;
- Verbot der Nutzung nicht-autorisierter Software, Apps, Netzwerke und Cloud-Dienste;
- Verbot der Nutzung eigener Software, Apps, Netzwerke, Clouds und Benutzeraccounts für dienstliche Zwecke.

Hinzu kommen noch solche Regelungen, die sich allgemein aus der dienstlichen Nutzung eines betrieblichen mobilen Geräts ergeben (s. o. II.2. u. 3.)

4. Rücknahme einer Erlaubnis

Wird die private Internet-Nutzung gestattet, liegt hierin grundsätzlich eine freiwillige Leistung des Arbeitgebers. Zur Klarstellung sollte der Arbeitgeber die Gestattung ausdrücklich unter den Vorbehalt der Freiwilligkeit stellen. Erst einmal entstandene Ansprüche des Arbeitnehmers, sei es durch Regelungen im Arbeitsvertrag, durch Betriebsvereinbarung oder durch betriebliche Übung, können ohne einen entsprechenden Vorbehalt nicht mehr ohne Weiteres zurückgenommen werden.

Formulierungsbeispiel:

„Dem Arbeitnehmer wird freiwillig und ohne Begründung eines Rechtsanspruchs gestattet, die am Arbeitsplatz vorhandenen Kommunikationsmittel – nach Maßgabe weiterer Anordnungen des Arbeitgebers – privat zu nutzen."

IV. Bring your own device

1. Begriff

Unter dem Begriff „Bring your own device", kurz auch „BYOD" genannt, versteckt sich das unternehmerische Ziel, Arbeitnehmern die dienstliche Nutzung ihrer privaten (i. d. R. mobilen) Geräte zu gestatten und diesen Zugriff auf die IT-Ressourcen des Unternehmens zu gewähren. Auf den ersten Blick hat dieses Verfahren einige Vorteile für beide Seiten. Der Arbeitnehmer kann ein (meist attraktives) Gerät seiner Wahl für private und dienstliche Zwecke einsetzen und benötigt kein weiteres mehr. Die hiermit einhergehende Zufriedenheit und Motivation des Arbeitnehmers kommt dem Arbeitgeber ebenso zugute, wie eine bessere Erreichbarkeit des Arbeitnehmers, der sein selbst ausgewähltes Gerät auch privat nutzt. Ob sich der Arbeitgeber wegen der vom Arbeitnehmer selbst gezahlten Geräte Kosten spart, mag unter Berücksichtigung des erforderlichen zusätzlichen Aufwandes für Administrations- und Sicherheitsmaßnahmen in Frage gestellt bleiben.