Bring Your Own Device (BYOD)

Rechtliche Probleme und Handlungsempfehlungen

Inhaltsverzeichnis

A. Hintergrund
B. Problematische Bereiche und Regelungsmöglichkeiten
I. Haftung
II. Arbeitsrecht
III. Datenschutz
1. Kontrollmöglichkeiten
2. Datengeheimnis
3. Technische und organisatorische Maßnahmen
4. Regelungsmöglichkeiten
IV. Urheberrecht
V. Aufbewahrungspflichten
VI. Geheimnisschutz und Strafrecht
VII. Beendigungstatbestände

A. Hintergrund

In den letzten Jahren ist der Absatz privater IT-Geräte deutlich angestiegen. Hier sind vor allem Laptops, Smartphones und Tablet-Computer zu nennen. Viele Arbeitnehmer bringen ihre privaten Geräte dabei immer häufiger mit an den Arbeitsplatz und möchten diese auch für dienstliche Aufgaben nutzen. Diese Einbindung privater Endgeräte für die dienstliche Nutzung bezeichnet man als „Bring your own device“, kurz „BYOD“. Hierbei steht der Begriff „device“ nicht nur entsprechend seiner Übersetzung für die IT-Endgeräte, sondern darüber hinaus auch für Software, Applikationen (kurz „Apps“), Datenbanken und Services.

Es zeichnet sich die Entwicklung ab, dass Arbeitnehmer ihre privaten Endgeräte in zunehmendem Maße auch dienstlich nutzen. Marketing Research Analysten sehen BYOD neben Cloud-Computing als den nächsten Megatrend in der IT-Branche. Arbeitgeber müssen sich also auf diese neue IT-Nutzung einstellen. Sobald man die dienstliche Nutzung der privaten Endgeräte erlaubt, erfordert dies zum einen auf rechtlicher Seite detaillierte Regelungen mit Arbeitnehmern und betroffenen Dritten und zum anderen müssen gewichtige technische und organisatorische Maßnahmen getroffen werden. Allen voran ist hierbei die unabdingbare Trennung von privaten und dienstlichen Daten zu nennen, welche sich mittels verschlüsselter Container (= verschlüsselte, abgeschlossene Bereiche auf einem Server; Container-Apps) oder Terminal-Lösungen bewerkstelligen lassen.

Die Untersagung der Einbringung privater Endgeräte für dienstliche Zwecke erscheint aufgrund der gegenwärtigen Entwicklungen nur noch in Ausnahmefällen möglich und auch nicht praktikabel. Durch eine bloße Duldung der dienstlichen Nutzung privater IT durch den Arbeitgeber schneidet sich dieser einerseits Einfluss- und Kontrollmöglichkeiten ab. Andererseits steht er vor erheblichen rechtlichen Problemen. Letztlich ist eine Umgestaltung eines etablierten Zustandes auch mit spürbarem Aufwand verbunden.

Mit der Nutzung privater Geräte gehen einige betriebswirtschaftliche Vorteile einher. Der Arbeitgebermuss seinen Beschäftigten keine eigenen Endgeräte zur Verfügung stellen, sondern zahlt stattdessen den Beschäftigten regelmäßig einen finanziellen Ausgleich für das Einbringen der eigenen Geräte. Gleichzeitig erlaubt der Arbeitgeber den Zugriff auf Informationssysteme und Daten mittels der privaten IT. Trotz des teilweise gezahlten Ausgleichs ergeben sich enorme Einsparpotenziale im Bereich der Beschaffung und Wartung der Geräte. Diese Kostensenkung ist jedoch nur ein Punkt, der für BYOD spricht. Daneben besteht nämlich eine deutliche Steigerung der Produktivität und Erreichbarkeit sowie ein sinkender Schulungsbedarf. Durch die Kopplung der privaten Endgeräte mit den Systemen des Arbeitgebers besteht auch nach Verlassen des Arbeitsplatzes die Möglichkeit, in gewohnter Weise weiterzuarbeiten. Gleichzeitig wird die Arbeit vereinfacht, da nur noch ein Gerät benutzt werden kann. Dadurch, dass der Arbeitnehmer bereits mit der Bedienung des Gerätes vertraut ist, führt BYOD zu einer Entlastung. Letztlich wird durch die Verwendung der privaten IT auch die Zufriedenheit der Beschäftigten und deren Identifikation mit dem Arbeitgeber erhöht.

Diesen Vorteilen stehen aber gewichtige Hindernisse rechtlicher, organisatorischer und technischer Natur gegenüber, die es zu bewerkstelligen gilt. Vor allem müssen die Bedenken der Mitarbeiter im Hinblick auf den unberechtigten Zugriff auf die Geräte und die darauf gespeicherten privaten Daten durch das Unternehmen oder dessen Fachabteilungen ausgeräumt werden. Dass einige Hürden vor der Einführung von BYOD bestehen, wird auch dadurch deutlich, dass sich einige Datenschutzaufsichtsbehörden kritisch bis gänzlich ablehnend zu der Frage geäußert haben, ob die Einführung von BYOD mit den rechtlichen Vorgaben überhaupt zu vereinbaren ist.

Zusammenfassend muss daher festgehalten werden, dass es rechtliche, technische und organisatorische Rahmenbedingungen überprüft werden müssen, bevor die Nutzung privater Geräte für dienstliche Zwecke zugelassen wird. Die Einführung von BYOD stellt letztlich eine betriebswirtschaftliche Entscheidung unter Abwägung der Vor- und Nachteile dar. Dabei sind auch Alternativen wie beispielsweise CYOD (choose your own device), bei der der Arbeitgeber die Endgeräte selbst anschafft, der Arbeitnehmer jedoch eine Auswahlmöglichkeit hat, denkbar.

B. Problematische Bereiche und Regelungsmöglichkeiten

Den oben angesprochenen Vorteilen von BYOD stehen gewichtige rechtliche Probleme gegenüber, die gegen eine Zulassung von BYOD durch den Arbeitgeber sprechen. Zu nennen sind hier zunächst die Haftung des Arbeitgebers bei auftretenden Schäden sowie datenschutz- und urheberrechtliche Aspekte. Des Weiteren sind Arbeits-, Handels-, Steuer- und Strafrecht von besonderer Bedeutung. Die Gesetze enthalten keine spezifischen Regelungen zu BYOD. Daneben ist – wie bisher ersichtlich – keine Rechtsprechung zu diesem Themenkomplex ergangen. Der rechtliche Rahmen muss daher durch BYOD-Richtlinien ausgestaltet werden. Sollte sich der Arbeitgeber zur Zulassung von BYOD entschließen, ist es unbedingt anzuraten, Regelungen über die genaue Ausgestaltung von BYOD mit den Mitarbeitern zu vereinbaren. Dabei wird es erforderlich sein, neben Dienst- und Betriebsvereinbarungen auch individuell arbeitsvertragliche Regelungen mit den Angestellten zu treffen.

I. Haftung

Haftungsprobleme können sich sowohl bezüglich der eingebrachten Geräte des Arbeitnehmers als auch für sensible Daten des Arbeitgebers ergeben. Sobald der Arbeitnehmer mit Zustimmung des Arbeitgebers private Endgeräte zur Dienststelle mitbringt und diese für dienstliche Zwecke einsetzt, besteht eine Schutzpflicht des Arbeitgebers für das vom Arbeitnehmer eingebrachte Eigentum.

Das besondere Risiko von BYOD im Bereich des Schadensrechts liegt aber vor allem darin, dass anders als auf dienstlichen Geräten möglicherweise nicht nur der Arbeitnehmer, sondern auch Dritte (erwachsene Familienangehörige, aber ggfs. auch minderjährige Kinder) Zugriff auf das Gerät haben. Des Weiteren wird die Zahl der heruntergeladenen Apps bzw. Programme auf einem Privatgerät größer als auf einem dienstlichen Gerät sein. Die Möglichkeit besteht, dass privat installierte Apps– vom Anwender unbemerkt – Zugriff auf E-Mail-Konten und dienstliche Datenbestände erhalten und vertrauliche Informationen nach außen leiten. Zudem dürfte die private Sicherheitssoftware schwächer oder zumindest nicht auf die auch dienstliche Verwendung abgestimmt sein. Folglich steigt die Gefahr der Infektion des Gerätes mit Schadsoftware. Dies kann im schlimmsten Falle zu einer Ausspähung von Dienstgeheimnissen oder einer Datenlöschung führen.

Ein Datenverlust kann durch regelmäßige Sicherungen zwar weitestgehend eingeschränkt werden, dennoch stellt sich die Frage nach der Haftung in Fällen der Ausspähung oder Löschung von dienstlichen Daten. Im Arbeitsrecht gibt es unter bestimmten Voraussetzungen eine Haftungsprivilegierung des Arbeitnehmers nach den Regeln des sog. innerbetrieblichen Schadensausgleichs, sodass dieser bei leichter oder mittlerer Fahrlässigkeit meist gar nicht oder nur teilweise haftet. Eine Mithaftung des Arbeitnehmers kommt beispielsweise im Falle der Umgehung

technischer Sicherheitsmaßnahmen oder aber bei Verstößen gegen dienstliche Benutzungsordnungen in Betracht. Dabei ist unklar und noch nicht gerichtlich entschieden, ob diese Privilegierung auch bei BYOD eingreift. Zu berücksichtigen ist aber, dass auf diesem Gebiet vieles vom Einzelfall abhängt. In der arbeitsgerichtlichen Rechtsprechung ist festzustellen, dass entsprechende Urteile sehr restriktiv sind, wenn es um Regelungen geht, die die Einschränkung des Privatlebens und der Freizeit von Arbeitnehmern betreffen. Somit besteht die Gefahr für den Arbeitgeber, den jeweiligen Mitarbeiter bei etwaigen Schäden nicht in Regress nehmen zu können.

Im Bereich des Telekommunikationsvertragsrechts kann es zu einer Vermengung von BYOD und Telearbeit kommen, wenn der Arbeitnehmer seinen privaten Internetanschluss für dienstliche Tätigkeiten nutzt. Die Angebote der Telekommunikationsanbieter differenzieren regelmäßig zwischen privater und geschäftlicher Nutzung, was sich auch im Entgelt niederschlägt. Der Arbeitnehmer wird nur einen Anschluss für die private Nutzung haben. Eine auch geschäftliche Nutzung wäre daher eine Vertragsverletzung des Arbeitnehmers. Diese kann den Telekommunikationsanbieter zum Schadensersatz oder zur Kündigung aus wichtigem Grund berechtigen.

Die Hardware bedarf der Wartung sowie der Reparatur und die Software regelmäßiger Updates, was grundsätzlich durch den Arbeitnehmer durchzuführen ist. Zur Vermeidung von Sicherheitslücken und Datenverlusten ist aber eine einheitliche Administration durch den Arbeitgeber zu empfehlen. In diesem Zusammenhang sollten betriebliche Vereinbarungen Informationen über die Haftung bei Verlust oder Beschädigung der Geräte oder betrieblicher Daten enthalten und eindeutig festlegen, wer Reparaturen in Auftrag gibt und deren Kosten trägt. Zudem sollte festgelegt werden, wer in welchen Konstellationen haftet und welche Partei unter welchen Voraussetzungen das Betriebsrisiko trägt. Außerdem ist dem Arbeitgeber eine regelmäßige Wartung der Privatgeräte anzuraten. Die ergänzende Verpflichtung des Mitarbeiters zur selbständigen Überprüfung des Geräts ist darüber hinaus empfehlenswert.

Es sollten ferner Regelungen über die dienstliche Nutzung und die weitere private Nutzung des Privateigentums des Arbeitnehmers getroffen werden. Gerade im Falle der Zahlung einer Vergütung für die betriebliche Nutzung der Geräte sollten auch Regelungen über die Mängelhaftung des Arbeitnehmers und die ihn treffenden Pflichten im Mangelfall getroffen werden. Der Arbeitgeber sollte für derartige Fälle Ersatzgeräte bereithalten. Ratsam ist auch die Regelung einer Benachrichtigungspflicht des Mitarbeiters, falls das private Gerät, auf dem dienstliche Daten gespeichert sind, gestohlen worden, verloren gegangen oder auf andere Weise abhandengekommen ist.

Es ist zu empfehlen, die Einstellung der Geräte-Konfiguration zentral vorzunehmen und die Arbeitnehmer im Rahmen einer Vereinbarung zu verpflichten, diese Einstellungen zu verwenden und nicht zu verändern. Dabei sollte der Zugriff auf das private Gerät von der Eingabe eines Passworts abhängig gemacht werden. Auch im Hinblick auf den Schutz von Betriebs- und Geschäftsgeheimnissen ist die verbindliche Vorgabe eines Passworts ratsam, zumal diese Daten oftmals vertraglichen Geheimhaltungspflichten gegenüber Dritten unterliegen. Selbstverständlich sollte die Verpflichtung des Arbeitnehmers auch beinhalten, dass er das Passwort gegenüber Dritten geheim hält und sicher aufbewahrt.

II. Arbeitsrecht

Bestehende Dienst- und Betriebsvereinbarungen umfassen regelmäßig nur die private Nutzung der Kommunikationssysteme des Arbeitgebers mittels dienstlicher Geräte und nicht die dienstliche Nutzung dieser Systeme über private Endgeräte. Daher sind im Falle der Zulassung von BYOD darüber hinausgehende Dienst- und Betriebsvereinbarungen notwendig. Dabei können unter anderem die datenschutzrechtlichen Belange der Mitarbeiter im Rahmen des § 26 Bundesdatenschutzgesetz (BDSG) geregelt werden, welcher die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses betrifft.

Aus arbeitsrechtlicher Perspektive ist im öffentlichen Sektor vor allem die Beteiligung des Personalrates von entscheidender Bedeutung. Eine Mitbestimmungspflicht bei der Einführung kann sich dementsprechend aus den §§ 75 Abs. 3 Nr. 15 (Regelung der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten), Nr. 16 (Gestaltung der Arbeitsplätze), Nr. 17 (Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen), 76 Abs. 2 Nr. 7 (Einführung grundlegend neuer Arbeitsmethoden) Bundespersonalvertretungsgesetz (BPersVG) und den entsprechenden Landespersonalvertretungsgesetzen ergeben.

Im nichtöffentlichen Bereich müssen die Vorschriften des Betriebsverfassungsgesetzes (BetrVG) beachtet werden. Zunächst hat der Betriebsrat ein Kontrollrecht nach § 80 BetrVG, wozu nach § 80 Abs. 1 Nr. 1 BetrVG auch die Überwachung der Einhaltung der zugunsten der Arbeitnehmer geltenden Gesetze zählt. Daneben kann sich eine Mitbestimmungspflicht des Betriebsrates aus § 87 Abs. 1 Nr. 1 (Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb), Nr. 2 (Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen sowie Verteilung der Arbeitszeit auf die einzelnen Wochentage) und Nr. 6 (Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen) BetrVG ergeben. Gegenstand dieses Mitbestimmungsrechts können beispielsweise der

Zeitpunkt der Einführung von BYOD, der Zeitraum der Nutzung und die überbetriebliche Vernetzung sein. Nach § 90 BetrVG bestehen im Hinblick auf die Planung von technischen Anlagen (§ 90 Abs. 1 Nr. 2 BetrVG), von Arbeitsverfahren und Arbeitsabläufen (§ 90 Abs. 1 Nr. 3 BetrVG) und der Arbeitsplätze (§ 90 Abs. 1 Nr. 4 BetrVG) Unterrichtungspflichten gegenüber dem Betriebsrat. Daher muss der Arbeitgeber den Betriebsrat bereits im Planungsstadium hinsichtlich der Gestattung von BYOD einbeziehen und diesen unter Vorlage der erforderlichen Unterlagen unterrichten.

Grundsätzlich ist der Arbeitgeber dazu verpflichtet, betriebliche Ressourcen bereitzustellen und zu erhalten. Erlaubt der Arbeitgeber die Einbringung eigener Geräte, ist es ratsam, die jeweiligen Gerätetypen und Softwareversionen genau zu bezeichnen und zu dokumentieren. Eines der größten Probleme im Zuge von BYOD ist nämlich die Verwaltung unterschiedlichster Mobilgeräte. Es ist daher eine hoch skalierbare Managementplattform erforderlich. Einer unbedingten Regelung bedarf im Zuge der Einführung von BYOD vor allem die konkrete Abgrenzung zwischen der privaten und betrieblichen Nutzung des eingebrachten Gerätes, insbesondere in zeitlicher Hinsicht. Im Rahmen der heutigen Kommunikation vermengen sich Freizeit und Arbeitszeit in einem zunehmenden Maße. BYOD-Programme verstärken diesen Effekt durch die permanente Erreichbarkeit des Arbeitnehmers, sodass sich der Arbeitnehmer gezwungen fühlen könnte, auch in seiner Freizeit dienstliche Anfragen auf seinem Gerät zu beantworten. Es sind daher klare und verlässliche Regelungen zum arbeitszeitlichen Umgang mit den privaten Geräten außerhalb der vereinbarten Arbeitszeit festzulegen. Insbesondere sind die Vorgaben für Ruhezeiten aus § 5 ArbZG bei einer entsprechenden Vereinbarung zu beachten. Die ständige Erreichbarkeit über das private Endgerät stellt nach überwiegender Auffassung zwar lediglich eine Rufbereitschaft dar, welche an sich noch nicht als Arbeitszeit zu werten ist. Rufbereitschaft bedeutet, dass sich der Arbeitnehmer verpflichtet, jederzeit für den Arbeitgeber erreichbar zu sein, um auf Abruf die Arbeit aufnehmen zu können. Sobald jedoch eine tatsächliche Arbeitsaufnahme stattfindet, handelt es sich um Arbeitszeit. Insofern sollte keine Verpflichtung des Arbeitnehmers zur ständigen Verfügbarkeit vereinbart werden. Davon abzugrenzen sind freiwillige Tätigkeiten des Arbeitnehmers außerhalb der regulären Arbeitszeit, welche nicht als Arbeitszeit gelten.

Auch der Vergütungsanspruch des Arbeitnehmers für die betriebliche Nutzung sollte vertraglich festgelegt werden. Entsprechend des Anteils der Nutzung sind die Kosten dort prozentual aufzuführen. Eine Anpassungsklausel ist daneben ratsam, um Veränderungen in der Verteilung dieser Anteile besser nachzukommen. Ebenso ist mit Hinblick auf Regelungen bezüglich des zeitlichen Umfangs an eine Vereinbarung zur Vergütung von Überstunden zu denken.

III. Datenschutz

Seit dem 25. Mai 2018 gilt die Datenschutzgrundverordnung (DSGVO) unmittelbar in den Mitgliedstaaten der Europäischen Union. Diverse Öffnungsklauseln der DSGVO ermöglichen den Mitgliedsstaaten allerdings den Erlass eigener Datenschutzvorschriften, insbesondere auch für den öffentlichen Bereich. So finden auf Hochschulen als öffentliche Stellen der Länder im Umkehrschluss aus § 1 Abs. 1 Nr. 2 BDSG auch weiterhin die Landesdatenschutzgesetze Anwendung. Dies gilt jedenfalls dort, wo die DSGVO keine abschließenden Regelungen trifft. Der Übersichtlichkeit halber erfolgt die Darstellung im Folgenden allerdings nicht anhand der Landesdatenschutzgesetze, sondern anhand des BDSG, das sich auch nach seiner Änderung inhaltlich weitestgehend mit den Datenschutzgesetzen der Länder deckt.

Werden private Endgeräte für dienstliche und nicht für private Zwecke genutzt, ist die DSGVO und das BDSG als Umkehrschluss aus Art. 2 Abs. 2 lit. c) DSGVO bzw. § 1 Abs. 1 S. 2 BDSG grundsätzlich auf den Arbeitgeber anwendbar, wenn dieser nicht eine solche Nutzung ausdrücklich und konsequent verbietet. Unterlässt er dies, sind Mitarbeiter datenschutzrechtlich dem Verantwortungsbereich des Arbeitgebers zuzurechnen, sofern sie in Ausübung ihrer arbeitsvertraglichen Pflichten handeln. Die Konsequenz daraus ist, dass die verarbeitende Stelle auch für den Datenumgang des Mitarbeiters auf dessen privaten Geräten verantwortlich ist, sofern personenbezogene Daten (gem. Art. 4 Nr. 1 DSGVO sind dies alle Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen) betroffen sind. Im Rahmen von BYOD ist der Arbeitnehmer als Teil der verantwortlichen Stelle aber nicht als Auftragsdatenverarbeiter im Sinne von Art. 28 DSGVO für den Arbeitgeber anzusehen.

1. Kontrollmöglichkeiten

Im Hinblick auf Kontrollmöglichkeiten des Arbeitgebers bei der dienstlichen Nutzung privater Geräte mangelt es an einschlägiger Rechtsprechung. Jedoch waren Rechtsprechung und Literatur sehr restriktiv hinsichtlich solcher Kontrollbefugnisse, wenn ein dienstliches Gerät auch im privaten Raum genutzt werden sollte. Legt man dies zugrunde, dann werden im erstgenannten Fall nur in seltenen Ausnahmefällen Kontrollmöglichkeiten des Arbeitgebers zu bejahen sein. Demgegenüber treffen aber sowohl die Leitung der verantwortlichen Stelle als auch den Datenschutzbeauftragten Kontrollpflichten. Diese können sich neben dem Datenschutzrecht auch aus gesellschafts-, handels- und steuerrechtlichen Pflichten ergeben.

Hinsichtlich der privaten Endgeräte steht dem Arbeitgeber kein originäres Zugriffs- bzw. Zugangsrecht zu. Daher muss ein solches und dessen Bedingungen mit dem Beschäftigten vertraglich vereinbart werden. Derartige individualvertragliche Vereinbarungen sind im Hinblick auf die

Grundrechte der Arbeitnehmer allerdings mit Risiken behaftet. Eine inhaltliche Beschränkung der Kontrollmaßnahmen im privaten Bereich auf das betrieblich absolut notwendigste Maß ist unumgänglich. Dies ist eine Konsequenz aus der oben erwähnten restriktiven Rechtsprechung der Arbeitsgerichte im privaten Lebensbereich der Arbeitnehmer. Besonderer Beachtung bedürfen Maßnahmen, welche gewährleisten, dass private Arbeitnehmerdaten nicht vom Arbeitgeber eingesehen werden.

Weiterhin zu beachten sind die Untersuchungsbefugnisse der Aufsichtsbehörde. Gem. Art. 51 Abs. 1 DSGVO hat jeder Mitgliedsstaat eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung der Verordnung einzurichten. Nach Art. 58 Abs. 1 lit. a) DSGVO hat die Aufsichtsbehörde z.B. die Befugnis, den Verantwortlichen anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Zudem kann die Behörde gem. Art. 58 Abs. 1 lit. b) DSGVO Untersuchungen in Form von Datenschutzüberprüfungen durchführen. Art. 58 Abs. 1 lit. e) DSGVO erlaubt es der Behörde weiterhin, von dem Verantwortlichen Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten. Schließlich kann die Aufsichtsbehörde nach Art. 58 Abs. 1 lit. f) DSGVO Zugang zu den Räumlichkeiten, einschließlich der Datenverarbeitungsanlagen und -geräte des Verantwortlichen verlangen. Wiederum im Hinblick auf die Grundrechte der Beschäftigten sind diese Untersuchungsbefugnisse im Rahmen der dienstlichen Nutzung privater IT problematisch, falls private Endgeräte der Aufsichtsbehörde vorgelegt werden müssen. Den Untersuchungsbefugnissen der Aufsichtsbehörde aus der DSGVO stehen hier insbesondere das Grundrecht auf Achtung des Privat- und Familienlebens gemäß Art. 7 Grundrechtecharta (GRCh) sowie das Grundrecht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh des Mitarbeiters entgegen. Es wird wohl im Einzelfall eine Interessenabwägung dahingehend erfolgen müssen, ob die Untersuchungsbefugnisse der Aufsichtsbehörde, welche die Einhaltung der Datenschutzgrundverordnung sicherstellen sollen, die genannten Rechte überwiegen.

Die soeben zu den Untersuchungsbefugnissen der Aufsichtsbehörde genannte Problematik gilt entsprechend für die Wahrnehmung der Aufgaben durch den behördlichen Datenschutzbeauftragten. Dieser hat gemäß § 7 Abs. 1 Nr. 2 Alt. 1 BDSG (und für den nichtöffentlichen Bereich gem. Art. 39 Abs. 1 lit. b) DSGVO) die Aufgabe, die Einhaltung der DSGVO bzw. des BDSG zu überwachen. Dies wird bei der Verwendung privater Endgeräte enorm erschwert.

Im nichtöffentlichen Bereich gilt für die Kontrolle durch die Aufsichtsbehörde neben den Vorschriften der DSGVO auch der § 40 BDSG. Nach § 40 Abs. 4 S. 1 BDSG haben die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Aus § 40 Abs. 5 S. 1 BDSG ergeben sich bezüglich der Grundstücke und Geschäftsräume der Stelle für die

Aufsichtsbehörde Befugnisse und Rechte zum Betreten und zum Zugang zu allen Datenverarbeitungsanlagen und -geräten. Diese Kontrollmaßnahmen sind erlaubt, soweit sie zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich sind. Noch nicht geklärt ist, ob und in welchem Umfang eine Aufsichtsbehörde im Zuge einer Betriebsprüfung beim Arbeitgeber auch private Endgeräte von Mitarbeitern oder deren Familienangehörigen, die Mitarbeiter überprüfen darf.

Im Hinblick auf Löschungspflichten ist aus datenschutzrechtlicher Sicht ferner darauf zu achten, dass solche Daten, zu deren Löschung die verantwortliche Stelle verpflichtet ist, auch auf dem Gerät des Arbeitnehmers gelöscht werden müssen.

2. Datengeheimnis

In § 5 S. 1 BDSG a.F. fand sich bisher das sog. Datengeheimnis, welches klarstellte, dass es den bei der Datenverarbeitung beschäftigten Personen untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. In der DSGVO findet sich eine solche Vorschrift zum Datengeheimnis nicht wieder. Das neue BDSG beinhaltet nur für die Verarbeitung personenbezogener Daten durch die für die Strafverfolgung zuständigen öffentlichen Stellen (vgl. § 45 S. 1 BDSG) eine entsprechende Verpflichtung auf das Datenschutzgeheimnis in § 53 BDSG. Allerdings greifen diverse Normen in der DSGVO(z.B. Art. 5, Art. 24, Art. 29 und Art. 32 DSGVO) das Datengeheimnis auf und lassen eine Verarbeitung personenbezogener Daten durch Beschäftigte nur nach den Vorgaben des verantwortlichen Arbeitgebers zu.

Benutzen neben dem Mitarbeiter auch Dritte – wie etwa Familienangehörige – das private Endgerät, so könnte eine Offenlegung der Daten durch Bereitstellung i.S.d. Art. 4 Nr. 2 DSGVO und damit eine Verarbeitung personenbezogener Daten vorliegen. Dies würde eine Verletzung geltenden Datenschutzrechts darstellen, da in einem solchen Fall weder eine Einwilligung noch ein anderer Erlaubnistatbestand einschlägig wäre. Des Weiteren ist zu beachten, dass die Kontrollmöglichkeiten des Arbeitgebers bei Nutzung privater Geräte zunächst stark eingeschränkt sind, sodass er kaum sicherstellen kann, dass betriebliche Daten nicht an Dritte weitergegeben werden.

Im Rahmen von BYOD sollte noch Art. 33 DSGVO beachtet werden. Nach Abs. 1 der Vorschrift sind Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung dem Verantwortlichen bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Diese Meldepflicht kann beispielsweise durch den Verlust eines privaten Endgerätes, auf dem einem Berufsgeheimnis unterliegende Daten gespeichert sind, ausgelöst werden.

3. Technische und organisatorische Maßnahmen

Gem. Art. 24 Abs. 1 DSGVO muss der Verantwortliche geeignete technische und organisatorische Maßnahmen umsetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt. Durch die dienstliche Nutzung privater Endgeräte besteht die Gefahr, dass die erforderliche Datensicherheit durch die Mitarbeiter nicht garantiert wird. Der zu fordernde Standard hängt einerseits stark von der Art der gespeicherten Daten ab, andererseits ist der Sicherheitsstandard der verwendeten IT entscheidend. Übliche kostenlose Anti-Virenprogramme oder Firewalls werden regelmäßig nicht ausreichen. Dabei wird ein relativer Ansatz verfolgt: je sensibler die Daten sind, desto eher ist eine Verarbeitung dieser Daten auf privaten Endgeräten unzulässig. Eine Zulässigkeit wird allenfalls dann bejaht, wenn der Arbeitgeber den Zutritt der zugelassenen Arbeitnehmer durch Kontrollmechanismen sowohl auf private als auch auf dienstliche Geräte gleichermaßen kontrollieren kann und umfassende Kontrollmöglichkeiten hinsichtlich der auf den Geräten gespeicherten dienstlichen Daten bestehen.

4. Regelungsmöglichkeiten

Es sollte mit jedem Arbeitnehmer eine Vereinbarung über den Einsatz der privaten Geräte für dienstliche Zwecke abgeschlossen werden. Um die genannten Gefahren einzudämmen, sollte sich der Arbeitgeber Kontrollrechte auf dem privaten Endgerät einräumen lassen, sodass der Verantwortliche und der Datenschutzbeauftragte seine Pflichten erfüllen können. Gleiches ist im Hinblick auf die Kooperationspflicht mit der Datenschutzaufsicht nötig. Inhaltlich sind dabei die Kontrollmaßnahmen im Sinne des Verhältnismäßigkeitsprinzips im privaten Bereich aufgrund der oben erwähnten restriktiven Rechtsprechung der Arbeitsgerichte auf das betrieblich absolut notwendigste Maß zu beschränken. Ein abgestufter Maßnahmenkatalog ist insofern ratsam. Oberste Priorität muss dabei den Maßnahmen zukommen, die gewährleisten, dass der Arbeitgeber keine privaten Daten zur Kenntnis nimmt. Durch die Nutzung privater Geräte zu dienstlichen Zwecken vermischt sich die private und dienstliche IT-Infrastruktur. Der Datenschutzbeauftragte ist grundsätzlich nicht zur Kontrolle der privaten IT berufen. Jedoch sollte er die Einhaltung des Datenschutzes auf privaten Geräten in dienstlicher Nutzung kontrollieren und die Ordnungsmäßigkeit der Anwendungen überwachen. Er verlässt aber den Bereich des Zulässigen, wenn er von privaten Daten Kenntnis erlangt, wie beispielsweise beim Einblick in private E-Mails.

Des Weiteren sollte klargestellt werden, dass eine Einsichtnahme durch Dritte in die sich auf dem Gerät befindlichen dienstlichen Daten unzulässig ist. Gleichzeitig muss der Arbeitgeber hier für die entsprechende technische Umsetzung sorgen (wie etwa verschlüsselte Container oder Terminal-Lösungen). Der Einsatz von Verschlüsselungssoftware ist unbedingt erforderlich. Für den Fall, dass der Mitarbeiter der Kontrolle durch den Arbeitgeber nicht zustimmt, sollte explizit ein Widerruf zur

Erlaubnis von BYOD vorbehalten werden. Es ist auch empfehlenswert, dem Arbeitnehmer für die dienstliche Nutzung geeignete Sicherheitssoftware zur Verfügung zu stellen, um die notwendige Datensicherheit zu gewährleisten. Dabei sind allerdings die oben in Kürze angesprochenen urheberrechtlichen Aspekte zu berücksichtigen.

Wie oben dargelegt ist ein Arbeitnehmer im Rahmen von BYOD nichts als Auftragsdatenverarbeiter des Arbeitgebers anzusehen. Dennoch ist es für den Arbeitgeber als Verantwortlichen verpflichtend, die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 24 DSGVO zu treffen, um die Datensicherheit und den Datenschutz zu gewährleisten, da Art. 24 DSGVO gerade für eine Verarbeitung durch die verantwortliche Stelle selbst (was bei einer Datenverarbeitung durch die Mitarbeiter der Fall ist) gilt. Zudem sollte der Arbeitnehmer zu deren Beachtung und Umsetzung schriftlich verpflichtet und regelmäßige Kontrollen vereinbart werden. Es ist also insgesamt ratsam, die Einzelheiten zur Gewährleistung der Datensicherheit zwischen Arbeitgeber und Arbeitnehmer vertraglich zu vereinbaren. Diese Regelung sollte auch Ausgestaltungen zur privaten Nutzung enthalten, was aufgrund der Verbindung und Vermischung von dienstlicher und privater Nutzung des Gerätes geboten erscheint. Neben den technischen Sicherungsmaßnahmen seitens des Arbeitsgebers sollte der Arbeitnehmer verpflichtet werden, dass unbefugte Dritte (etwa Ehepartner, Lebenspartner, Kinder, Freunde oder Bekannte) keinerlei Zugriff auf Unternehmensdaten haben. Darüber hinaus sollten klare Regelungen hinsichtlich der Nutzung des Gerätes bei privaten oder dienstlichen Reisen ins Ausland getroffen werden, da beispielsweise die Sicherheitsorgane einiger Länder (insbesondere die Finanzbehörden) zum Zugriff auf private Daten berechtigt sind.

Die privaten Daten auf den Geräten der Mitarbeiter sind deren Privatsphäre zuzuordnen und daher vor dem Zugriff durch den Arbeitgeber geschützt. Der Arbeitgeber muss aber die betrieblichen Daten auf diesen Geräten nutzen, bearbeiten und löschen können. Daher sind dahingehende Regelungen mit den Arbeitnehmern zu vereinbaren. Eine Löschung privater Daten seitens des Arbeitgebers sollte dabei nur für Notfälle vorgesehen werden. Neben den vertraglichen Regelungen wird dazu geraten, auf technischer Ebene den Arbeitnehmer zur Trennung von privaten und dienstlichen Daten auf dem Endgerät zu verpflichten. Denkbar wäre hier die Konfiguration virtueller Desktops, die Partitionierung der Festplatten der Geräte, verschlüsselte Container (Container-Apps) oder Terminal-Lösungen. Auf diese Weise kann einerseits eine Kontrolle erfolgen, ohne dass private Daten des Arbeitnehmers betroffen wären. Andererseits könnte illegal installierter Software der Zugriff auf das Unternehmensnetzwerk verweigert werden. Auch für weitere Elemente der IT-Struktur (Firewalls, Spam- und Virenschutz, Serververwaltung) könnte die technische Aufteilung des privaten Endgeräts eine Lösungsmöglichkeit darstellen.

Generell sollte daneben die Nutzung der betrieblichen Daten auf dem privaten Gerät über einen gesicherten Fernzugriff erfolgen. Im Hinblick auf die lokale Speicherung von Daten sollte vereinbart werden, ob und wie dienstliche Daten auf den privaten Geräten der Arbeitnehmer gespeichert werden, da dadurch der Zugriff des Arbeitgebers auf die Daten erheblich erschwert wird. Aus denselben Gründen sollten auch private und dienstliche E-Mails voneinander getrennt in separaten Ordnern oder Containern abgespeichert werden. Konkrete Handlungsanweisungen und Vereinbarungen mit den Arbeitnehmern sollten die technischen Vorkehrungen flankieren, um vor allem auch den Schutz der personenbezogenen Daten, welche verarbeitet werden, zu gewährleisten.

Auch die immer populärer werdenden Cloud-Dienste stellen ein Risiko im Rahmen von BYOD dar. Der Arbeitgeber sollte die privaten Geräte vor der Freigabe für die betriebliche Nutzung auf die dort vorhandenen Cloud-Dienste und deren Konfiguration überprüfen. In diesem Zuge sollten automatische Backups betrieblicher Daten in der Cloud unterbunden werden. Genauso sollte mit Backups auf privater Hardware des Arbeitnehmers verfahren werden, die der Kontrolle des Arbeitgebers entzogen sind.

IV. Urheberrecht

Der Arbeitnehmer bleibt bei der Einbringung seiner Geräte samt Software deren Eigentümer. Dies gilt auch im Falle der betrieblichen Nutzung. Die Nutzungsrechte an der installierten Software sind aber von der Eigentumslage zu unterscheiden.

Sobald der Arbeitnehmer private Endgeräte mit installierter Software für dienstliche Zwecke nutzt, können der Arbeitgeber und der Arbeitnehmer in Konflikt mit dem Urheberrecht kommen. Bei jedem Einsatz von Software müssen die entsprechenden Nutzungsrechte eingehalten werden. Die Nutzungsrechte beziehen sich oft aber nur auf eine bestimmte Nutzungsart. Die auf dem privaten Endgerät installierte Software ist häufig nur auf die private Nutzung ausgerichtet und daher vom Hersteller ausschließlich zu diesem Zweck lizenziert. Die Lizenzbedingungen sehen in diesem Fall regelmäßig eine dienstliche Nutzung der Software nicht vor. Anbieter von Freeware und Cloud-Anwendungen sehen in ihren Lizenzbedingungen üblicherweise besondere Modelle für die dienstliche Nutzung vor. Entsprechendes kann auch im umgekehrten Fall gelten, wenn also die durch den Unternehmer lizenzierte Software auf den privaten Geräten installiert wird.

Häufig wird der Arbeitnehmer die für die dienstliche Nutzung lizenzierte Software privat nutzen und umgekehrt für private Zwecke erworbene Software auch für dienstliche Angelegenheiten einsetzen. Dadurch kann es zu verbotenen und strafbaren Verhaltensweisen in Form von vergütungsrelevanten Nutzungshandlungen sowie urheberrechtlich relevanten Vervielfältigungen und Weitergaben kommen. In diesem Zusammenhang kann gerade die dienstliche Nutzung der Software als solche die

Verletzungshandlung darstellen. Zur Kontrolle und zum Ausschluss einer Unterlizenzierung seitens des Arbeitgebers sind daher regelmäßige interne Audits unabdingbar. Weitaus gefährlicher als diese Unterlizenzierung ist aber die Verwendung von illegaler Software aus zweifelhaften Quellen. Aufgrund der erhöhten Anfälligkeit für Hacker- oder Virenangriffe droht bei Verwendung dieser Software eine erhöhte Gefahr für die IT- und Unternehmenssicherheit.

Die oben beschriebenen Handlungen können je nach Konstellation für Arbeitgeber und Arbeitnehmer erhebliche zivilrechtliche Folgen haben. So besteht zunächst ein Anspruch auf Schadensersatz und Unterlassung gegen die handelnde Person aus § 97 UrhG. Nach § 99 UrhG haftet auch der Unternehmer für die Urheberrechtsverletzungen seiner Mitarbeiter. „Unternehmer“ i. S. d. § 99 UrhG sind dabei auch Körperschaften des öffentlichen Rechts, also z. B. Hochschulen. Zu beachten ist zudem die Strafvorschrift des § 106 UrhG, die für rechtswidrige Vervielfältigungshandlungen eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vorsieht.

Um das Risiko der Haftung für Urheberrechtsverletzungen zu minimieren, sollte das betriebliche Lizenzmanagement auf die privaten Geräte in betrieblicher Nutzung erstreckt werden. Idealerweise müsste man die Geräte der Mitarbeiter regelmäßig auf illegale oder unlizenzierte Software überprüfen. Dies könnte in einer Betriebsvereinbarung geregelt werden. Es erscheint jedoch unwahrscheinlich, dass ein Mitarbeiter den gesamten Inhalt seines Gerätes ohne weiteres offenlegen wird. Alternativ könnte man von dem Mitarbeiter in regelmäßigen Abständen fordern, einen Nachweis über die ordnungsgemäße Lizenzierung der von ihm zu betrieblichen Zwecken eingesetzten Software zu erbringen. Diesen Nachweis könnte man durch eine stichprobenartige Überprüfung absichern, vorausgesetzt der Mitarbeiter hat sein Einverständnis dazu erklärt. Es wäre eine Regelung denkbar, dass im Falle einer Weigerung das private Gerät nicht betrieblich verwendet werden darf. Eine sehr strikte Regelung könnte daneben vorsehen, welche Software der Mitarbeiter auf seinem Endgerät installieren darf und dass dahingehende Kontrollen erlaubt sind. Gewährleistungsansprüche für die eingesetzte Software könnten an den Arbeitgeber abgetreten oder für den Arbeitnehmer geltend gemacht werden. Die internen IT-Richtlinien sollten auf die Lizenzneuerungen im Zuge von BYOD angepasst und deren Einhaltung regelmäßig überprüft werden.

V. Aufbewahrungspflichten

Betriebliche Dokumente müssen revisionssicher archiviert werden. Daher sind eine Vielzahl von gesetzlichen Aufbewahrungspflichten (z.B. § 257 HGB, § 147 AO, diverse Vorgaben aus den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)) zu beachten, die zwingende steuer- und bilanzrechtliche Vorgaben an die Dokumentation von Geschäftsvorgängen aufstellen.

Insofern müssen Vereinbarungen mit dem Arbeitnehmer getroffen werden, die sicherstellen, dass diesen Archivierungspflichten nachgekommen wird, selbst wenn Geschäftsvorgänge über private Endgeräte abgewickelt werden.

Dabei sollte durch Regelungen ausgeschlossen werden, dass geschäftsrelevante Aufzeichnungen, vor allem geschäftliche E-Mails, nicht nur im privaten Bereich des Endgerätes be- und verarbeitet werden, sodass sie am Arbeitgeber vorbeilaufen. Es ist nämlich zu beachten, dass es zur Erfüllung von Aufbewahrungspflichten notwendig ist, die Daten nicht nur auf dem Endgerät des Arbeitnehmers, sondern zusätzlich beim Arbeitgeber zu speichern. Darüber hinaus müsste beispielsweise die Finanzverwaltung für eine Überprüfung jederzeit unmittelbaren Zugriff auf alle privaten Geräte der Mitarbeiter erhalten.

VI. Geheimnisschutz und Strafrecht

Neben dem Schutz von personenbezogenen Daten ist im Zuge von BYOD der Schutz von Betriebs- und Geschäftsgeheimnissen in Form eigener und fremder Unternehmensdaten sowie der Schutz von Privatgeheimnissen Dritter zu berücksichtigen. Die Sicherheitsmaßnahmen auf den privaten Geräten werden meist unter denen der dienstlichen Geräte liegen. Dies führt regelmäßig zu einer Offenbarung gegenüber Providern und anderen Dritten. Damit rücken die Straftatbestände des Ausspähens von Daten nach § 202a StGB und des Abfangens von Daten nach § 202b StGB durch Dritte in den Fokus. Durch die Einbindung privater Endgeräte in die Kommunikationssysteme des Arbeitgebers sind ggfs. auch die §§ 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten), 203 StGB (Verletzung von Privatgeheimnissen) und 303a StGB (Datenveränderung) von Bedeutung. Genauso kann sich aber der Arbeitgeber selbst gem. § 202a StGB oder gem. § 303a StGB strafbar machen, wenn er mittels Fernzugriff Daten des Arbeitnehmers löscht oder verändert. Um dies zu vermeiden, kann nur noch einmal auf die essentielle Bedeutung der Trennung von privaten und dienstlichen Daten mittels entsprechender technischer Maßnahmen hingewiesen werden. Denn hinsichtlich des Zugriffs auf dienstliche Daten kann sich der Arbeitgeber nicht strafbar machen. Besondere Aufmerksamkeit muss dem Fall gewidmet werden, dass das Gerät des Arbeitnehmers abhandenkommt und zur Abwehr unbefugter Zugriffe eine Löschung aller Daten per Fernzugriff erfolgt. Dadurch werden auch private Daten gelöscht. Daher muss entweder ein eindeutiges Einverständnis des Arbeitnehmers vorliegen, welches die Rechtswidrigkeit der Tat entfallen lässt, oder der Löschungsvorgang ist technisch so auszugestalten, dass wiederum keine privaten Daten erfasst werden. Auch im Rahmen von BYOD ist somit das Ausspähen, Abfangen und Verändern von Daten strafbar.

Daneben sind die wettbewerbsrechtlichen Vorschriften der §§ 17, 18 UWG zu berücksichtigen. Dienstliche Daten können Betriebs- bzw. Geschäftsgeheimnisse darstellen. Diese sind definiert als jede im Zusammenhang mit einem Geschäftsbetrieb stehende nicht offenkundige, sondern nur einem begrenzten Personenkreis bekannte Tatsache, an deren Geheimhaltung der Unternehmensinhaber ein berechtigtes wirtschaftliches Interesse hat und die nach seinem bekundeten oder doch erkennbaren Willen auch geheim bleiben sollen.

Mit der Vergegenwärtigung und Einhaltung des gesetzlichen Rahmens gehen zwei Vorteile einher: Einerseits hilft es bei dem technischen Schutz vor Missbräuchen, andererseits unterstützt es die Einführung und Umsetzung von BYOD.

VII. Beendigungstatbestände

Das Endgerät steht im Eigentum des Arbeitnehmers. Die dort abgespeicherten Daten sind teilweise nicht eindeutig dem privaten oder dienstlichen Bereich zuzuordnen. Daher sollten vor allem zur Vermeidung von Unklarheiten die Beendigungstatbestände von BYOD in die Vereinbarung zwischen Arbeitnehmer und Arbeitgeber aufgenommen werden. Zu denken wäre hierbei an eine Befristungsregelung (etwa für eine Erprobungsphase), an ein Widerrufsrecht oder an ein Kündigungsrecht. Gleichwohl sollten in einer solchen Vereinbarung Regelungen zur Aushändigung der betrieblichen Daten an den Arbeitgeber nach Beendigung des Arbeitsverhältnisses getroffen werden. Aus ihr muss deutlich hervorgehen, welche Daten vom Arbeitnehmer an den Arbeitgeber herauszugeben sind und welche Dateien und Dateikopien rückstandslos gelöscht werden müssen. Für Notfälle sollte, wie bereits erwähnt, eine Möglichkeit zur Löschung per Fernzugriff vereinbart werden.

Stand Juni 2020

Forschungsstelle Recht im DFN

Die Forschungsstelle Recht ist ein Projekt an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung unter der Leitung von Prof. Dr. Thomas Hoeren, Leonardo-Campus 9, D-48149 Münster, E-Mail: recht@dfn.de