Dr. iur. Lorenz Franck, Bonn*

Bring your own device – Rechtliche und tatsächliche Aspekte

Die Verwendung mitarbeitereigener Hardware im Unternehmen ist zwischenzeitlich zum Trendthema avanciert. Der nachfolgende Beitrag soll einen großräumigen Überblick über die akuten Fragestellungen aus IT-Sicherheit, Datenschutzrecht und anderen Rechtsbereichen bieten.

I. Problemaufriss

Privat angeschaffte Geräte sollen für dienstliche Zwecke oder jedenfalls in Verbindung mit der Unternehmensinfrastruktur verwendet werden. Nach Umfragen des BITKOM-Verbandes verwenden bereits 71 % der Beschäftigten in Deutschland ihre eigenen Geräte für den Beruf. In 21 % der Unternehmen wird diesen Geräten Zugriff auf die IT-Infrastruktur gewährt[1]. Nach einer Umfrage des Marktforschungsunternehmens Gartner wollen 38 % aller befragten Unternehmen bis 2016 vollständig und verpflichtend auf BYOD setzen[2]. Das Thema hat es aus der IT-zentrischen Sphäre bereits in die Tagespresse geschafft[3].

Für ein derartiges Vorhaben kommen verschiedene Motivationen in Betracht. Zum Teil möchte die Geschäftsleitung hochpreisig bezahlte Vorzeigegeräte einsetzen und weist die IT-Abteilung an, diese Geräte in die Unternehmens-IT einzubinden[4]. Zum Teil soll die Zufriedenheit der Mitarbeiter und ihre Bindung an das Unternehmen gesteigert werden[5]. Hier spielen die Gewöhnung an konkrete Hard- und Softwarekombinationen, das Prestige gewisser Marken und die Pflege von gleichermaßen beruflichen und privaten Kontakten vermittels desselben Gerätes eine Rolle.

Mancherorts versprechen sich Unternehmen auch finanzielle Einsparungen, wenn die Mitarbeiter für Anschaffung und Wartung der Geräte aufkommen[6]. Zumindest beim Hardwarehersteller IBM hat sich diese Erwartung allerdings nicht erfüllt[7].

Zumeist fällt das Schlagwort „BYOD“ in einem Atemzug mit Consumer-Grade-Geräten wie Notebooks, Tablets und Smartphones. Insoweit wird auch von einer „Consumerization“ der Unternehmens-IT gesprochen[8]. Das Gefahrenpotential gerade von mobilen Geräten ist dabei hoch. Hierauf sammeln sich die Daten von Mitarbeitern, Kunden und des Unternehmens selbst. Hierunter können sich also personenbezogene und telekommunikationsbezogene Informationen sowie Geschäftsgeheimnisse befinden.

Erforderlich ist daher ein Datenschutz- und Datensicherheitskonzept, welches den damit verbundenen Risiken angemessen Rechnung trägt. Insbesondere ist die Anlage zu § 9 S. 1 BDSG mit den darin zugrundegelegten Grundpflichten zu beachten. Weiterhin ergeben sich arbeitsrechtliche, urheberrechtliche, handelsrechtliche, steuerrechtliche und sogar strafrechtliche Fragestellungen.

II. Sicht der Aufsichtsbehörden

Die Datenschutzbeauftragten der Länder äußern sich nach wie vor verhalten zu BYOD. Noch 2009 ging das ULD Schleswig-Holstein davon aus, dass die konsequente Einhaltung technisch-organisatorischer Maßnahmen auf privaten Endgeräten eigentlich gar nicht möglich sei[9]. In Mecklenburg-Vorpommern wird momentan geraten, private Geräte so restriktiv wie möglich zu handhaben[10]. Der Hessische Datenschutzbeauftragte hat jüngst eine allgemeine technische Handreichung zur Benutzung von Smartphones und Tablets veröffentlicht, hält die rechlichen und tatsächlichen Widrigkeiten beim Einsatz spezifisch-mitarbeitereigener Hardware derweil für unüberwindbar[11]. In Berlin wird eindringlich vor den Gefahren von BYOD

* Der Autor ist Rechtsreferendar bei der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) in Bonn.

1 BITKOM, Mitarbeiter verwenden ihre privaten Geräte für den Job, online unter bitkom.org/de/themen/54633_75801.aspx.

2 Gartner, Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes, online unter gartner.com/newsroom/id/2466615.

3 Dommer/Finsterbusch, Betriebsgeheimnis auf dem Smarphone, FAZ vom 28.03.2013, online unter http://faz.net/-gym-77up2.

4 Hemker, DuD 2012, 165.

5 Göpfert/Wilke, NZA 2012, 765; Herrnleben, MMR 2012, 205; Weiß/Leimeister, Wirtschaftsinformatik 2012, 351; Zöll/Kielkowski, BB 2012, 2625.

6 Göpfert/Wilke, NZA 2012, 765; Heinzelmann, DSB 2012, 11; Imping/Pohle, K&R 2012, 470; Zöll/Kielkowski, BB 2012, 2625. Kritisch zum Einsparpotential dagegen Schuld, Versicherungswirtschaft 2013, 10 und Weiß/Leimeister, Wirtschaftsinformatik 2012, 351, 354.

7 Bergstein, IBM Faces the Perils of „Bring Your Own Device“, Technology Review, online unter technologyreview.com/news/427790/ibm-faces-the-perils-of-bring-your-own-device. Zu den Kosten siehe auch unten IV.4 und 5.

8 Heinzelmann, DSB 2012, 11; Hemker, DuD 2012, 165.

9 ULD Schleswig-Holstein, Tätigkeitsbericht 2009, (= LT-Drs. 16/2439), S. 115, online unter datenschutzzentrum.de/material/tb/tb31/31_Taetigkeitsbericht.pdf.

10 LfDI Mecklenburg-Vorpommern, „Bring Your Own Device“ (BYOD) – ist ein datenschutzgerechter Einsatz von Smartphones und Tablet PC's möglich?, online unter http://www.lfd.m-v.de/online_tb/byod.html.

11 Hessischer DSB, Handreichung zur Nutzung von Smartphones und Tablet-Computern in Behörden und Unternehmen, 2013, S. 16, online unter http://www.datenschutz.hessen.de/tf015.htm.

gewarnt und dessen Einführung zumindest für den Bereich der öffentlichen Verwaltung für unzulässig erklärt[12]. Eine gemeinsame Stellungnahme etwa des Düsseldorfer Kreises fehlt bislang[13].

Das sachverwandte Bundesamt für Sicherheit in der Informationstechnik (BSI) hält die datenschutzkonforme Nutzung mitarbeitereigener Hardware durchaus für möglich, mahnt aber mit Nachdruck verantwortliches Handeln an[14]. Es ist davon auszugehen, dass die Fragestellungen rund um BYOD demnächst in den IT-Grundschutzkatalog des BSI einfließen werden.

III. Datenschutzrecht

1. Auftragsdatenverarbeitung

Umstritten ist zunächst, ob die Verwendung mitarbeitereigener Hardware einer Auftragsdatenverarbeitung nach § 3 VII BDSG gleichkommt und damit einen formbedürftigen Vertrag nach § 11 II BDSG voraussetzt.

Für die Verwendung privater Geräte durch selbständige Unternehmer mag dies zutreffen[15]. Allerdings ist das bereits unabhängig von den Eigentumsverhältnissen der Hardware der Fall.

Ein Teil der Literatur geht stattdessen pauschal von einer Auftragsdatenverarbeitung aus, wenn private Geräte eingesetzt werden[16]. Dem wird berechtigterweise widersprochen, wenngleich mit zum Teil zweifelhaften Argumenten. So kann etwa auch eine Privatperson Partei eines ADV-Vertrages sein[17]. Die begriffliche Unterscheidung zwischen Auftragsdatenverarbeitern nach § 3 VII BDSG und den bei der Datenverarbeitung beschäftigen Personen nach § 5 S. 1 BDSG besitzt lediglich Indizwirkung, ebenso jene Differenzierung in Art. 2 lit. f) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates[18].

Überzeugend ist hingegen die spezifische Rechtsbeziehung zwischen Arbeitgeber und Arbeitnehmer. Der Mitarbeiter bleibt in datenschutzrechtlicher Beziehung Teil der verantwortlichen Stelle[19]. Eine Risikoerhöhung oder ein etwaiger Verstoß gegen technisch-organisatorische Maßnahmen macht den Mitarbeiter nicht plötzlich zum eigenständigen Datenverarbeiter. Für eine analoge Anwendung des § 11 II BDSG fehlt es an jedweder Regelungslücke.

Vermittelnd geben einige Autoren zu bedenken, dass der Arbeitgeber auch ohne Rückgriff auf Vorschriften über die Auftragsdatenverarbeitung zur Einhaltung der technisch-organisatorischen Maßnahmen nach § 9 S. 1 BDSG nebst Anlage verpflichtet bleibt[20]. Im Hinblick auf etwaige Kontrollrechte oder die (immerhin dem Vorbehalt des Gesetzes unterworfene) Ahndung datenschutzrechtlicher Verstöße ist dadurch jedoch nichts gewonnen. Im Interesse der Rechtssicherheit ist also die Annahme einer Auftragsdatenverarbeitung im Zusammenhang mit BYOD strikt abzulehnen.

2. Technisch-organisatorische Maßnahmen

Der Arbeitgeber ist als verantwortliche Stelle der Anlage zu § 9 S. 1 BDSG verpflichtet. Bei den zumeist mobilen Geräten ist eine zweckmäßige Zutrittskontrolle allderdings kaum möglich. Umso mehr müssen wirksame Kontrollen von Zugang, Zugriff, Eingabe und Weitergabe implementiert werden. Ein entsprechendes Identitätsmanagement[21] dient der Eingabekontrolle, Synchronisations- und Backup-Tools gewährleisten die dauerhafte Verfügbarkeit der Daten. Private und betriebliche Daten sind zwingend zu separieren[22]. Geeignete Verschlüsselungsmethoden sind sowohl auf dem Gerät selbst als auch zwischen Gerät und Unternehmens-IT einzusetzen.

a) Organisation

Zu den organisatorischen Maßnahmen gehört eine entsprechende (Nach-)Schulung der Arbeitnehmer. Für BYOD kommen ausschließlich solche Geräte in Betracht, die im Alleineigentum des jeweiligen Arbeitnehmers stehen[23]. Die Mitarbeiter müssen angewiesen werden, geeignete Passwörter zu generieren und sicher zu verwalten. Die Weitergabe des Gerätes an Dritte (auch an Familienangehörige) ist zu untersagen[24]. Zu-

12 Berliner Beauftragter für Datenschutz und Informationsfreiheit, Bericht 2012, S. 32, online unter http://www.datenschutz-berlin.de/content/nachrichten/datenschutznachrichten/27-maerz-2013.

13 Lediglich zur Smartphonebenutzung als solcher existiert ein entsprechener Beschluss, dieser bezieht sich jedoch im Wesentlichen auf arbeitnehmerdatenschutzrechtliche Fragestellungen, Beschl. v. 04./05. Mai 2011, online unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/00500 52011SmartphoneNutzung.html.

14 BSI, Überblickspapier Consumerization und BYOD, 2013, S. 7 f., online unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf gibt spezifische Handlungsanweisungen.

15 Hierzu Conrad/Schneider, ZD 2011, 153, 154; Imping/Pohle, K&R 2012, 470, 473.

16 So Koch, ITRB 2012, 35, 39, wenngleich ohne jegliche Begründung. Zöll/Kielkowski, BB 2012, 2625 verstehen dies bestenfalls als analoge Anwendung des § 11 BDSG.

17 Irrig insoweit Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 26.

18 Kremer/Sander, ITRB 2012, 275, 278.

19 Conrad/Schneider, ZD 2011, 153, 154; Kremer/Sander, ITRB 2012, 275, 277 f.; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 26; Zöll/Kielkowski, BB 2012, 2625.

20 Conrad/Schneider, ZD 2011, 153, 154; Imping/Pohle, K&R 2012, 470, 473; Kremer/Sander, ITRB 2012, 275, 278.

21 Vielen Consumer-Geräten fehlt es heute wieder an Mehrbenutzerfunktionalität, siehe auch Kremer/Sander, ITRB 2012, 275, 279.

22 Arning/Moos/Becker, CR 2012, 592, 595; Bierekoven, ITRB 2012, 106, 107; BITKOM, Bring Your Own Device, 2013, S. 6, online unter www.bitkom.org/de/themen/50792_75275.aspx; Göpfert/Wilke, NZA 2012, 765, 766; Zöll/Kielkowski, BB 2012, 2625.

23 Im Miteigentum stehende, geleaste, leihweise überlassene oder aber unter Eigentumsvorbehalt finanzierte Geräte sind der wirksamen rechtlichen und tatsächlichen Kontrolle durch die verantwortliche datenverarbeitende Stelle entzogen.

24 So die wohl h.M., vgl. Berliner BDI (Fn. 12), Bericht 2012, S. 35; BITKOM (Fn. 22), BYOD 2013, S. 6; Hörl, ITRB 2012, 258, 260. Conrad/Schneider, ZD 2011, 153, 158 halten ein derartiges Verbot indes für unwirksam. Bierekoven, ITRB 2012, 106, 107 hält die Weitergabe an Familienangehörige jedenfalls für üblich.

gleich ist in Anlehnung an die Skandalisierungspflicht nach § 42a BDSG auf zeitnahe Verlustanzeigen hinzuwirken[25]. Unternehmens- und Mitarbeiterdaten dürfen von den Usern nicht eigenmächtig vermischt werden. Die Mitarbeiter müssen sich um einen wirksamen Malwareschutz und regelmäßige Updates bemühen, sofern dies nicht bereits automatisiert geschieht. Cloud-Services sind tabu, ebenso File-Sharing-Applikationen. Die Installation unlizenzierter bzw. unzertifizierter Software, ggf. mittels eines sog. Jailbreaks, stellt ein weiteres Sicherheitsrisiko dar und ist zu unterlassen[26].

b) Technik

Die technischen Sicherungsmaßnahmen können nicht losgelöst vom konkreten Anwendungsfall betrachtet werden. Stichpunktartig sei aber auf die Verwendung von Verschlüsselungssoftware, Synchronisationssoftware, Sandboxing, Data-Loss-Prevention, Theft-Recovery, Remote-Wipe, VPN, Remote-Desktop-Applikationen u.ä. hingewiesen. Eine Reihe dieser Funktionaliäten firmiert heute gebündelt unter dem Begriff Mobile Device Management (MDM). Dieses wird von verschiedenen Herstellern für eine Reihe mobiler Plattformen angeboten und ermöglicht eine zentrale Verwaltung der Sicherheitsfeatures im Unternehmen[27]. Die Geeignetheit der jeweiligen MDM-Lösung ist vor ihrem Einsatz eingehend zu überprüfen.

3. Kontrollrechte

Auch abseits der Auftragskontrolle in der Anlage Nr. 6 zu § 9 S. 1 BDSG ist die Einhaltung des Datenschutzniveaus zu prüfen. So besitzt der betriebliche Datenschutzbeauftragte gemäß § 4g I S. 1 BDSG und den entsprechenden Ländergesetzen eigene Kontrollbefugnisse. Die zuständige Aufsichtsbehörde besitzt z.B. nach § 38 IV BDSG Prüfungs- und Betretungsrechte (letztere freilich nur für Räumlichkeiten der verantwortlichen Stelle, ggf. müssen die mobilen Devices dorthin verbracht werden). Hinzu kommen originäre Kontrollpflichten des Arbeitgebers nach datenschutz-, handels- und steuerrechtlichen Vorschriften[28]. Fachaufsichtsbehörden sind überdies zu berücksichtigen.

Die gesetzlich vorgesehen Kontrollmöglichkeiten müssen auch bei Einführung von BYOD erhalten bleiben[29]. Eine Verweigerung von Kontrollmaßnahmen muss dagegen zwangsläufig zur Beendigung des BYOD-Programms führen[30].

4. Arbeitnehmerdatenschutz

Bei alledem dürfen die personenbezogenen Daten des jeweiligen Mitarbeiters nicht aus den Augen verloren werden. Den Beschäftigten schützt dabei nicht allein § 32 BDSG als Konkretisierung des Allgemeinen Persönlichkeitsrechts, sondern zugleich auch das parallel gelagerte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Beide Grundrechtsgehalte werden jeweils abgeleitet aus den Artt. 1 I, 2 I GG.

Die durchzuführenden Kontrollen sollten daher auf ein Mindestmaß reduziert werden[31]. Die Erhebung privater Dateiinhalte durch den Arbeitgeber ist im Zweifel nicht erforderlich zur Durchführung des Beschäftigungsverhältnisses[32]. Dennoch ermöglicht MDM die Erhebung, Löschung, Sperrung und Veränderung auch privater Informationen[33]. Ist zugleich eine Theft-Recovery mittels GPS-Koordinaten implementiert, entstehen zwangsläufig Bewegungsprofile[34]. Der Beschäftigte muss auf seine diesbezüglichen Rechte zunächst wirksam verzichten, bevor er private Hardware im Beruf nutzen kann.

IV. Arbeitsrecht

1. Individualvereinbarung

Es bedarf einer wirksamen vertraglichen Regelung zwischen Arbeitgeber und Arbeitnehmer. Diese muss nicht nur BDSG- sondern auch AGB-fest sein, sie darf also den Beschäftigten nicht unangemessen benachteiligen. Nach dem in § 307 I S. 2 BGB niedergelegten Transparenzgebot müssen sich die Rechte und Pflichten des Arbeitnehmers unzweifelhaft aus der Vereinbarung ergeben. Unklarheiten gehen gemäß § 305c II BGB zu Lasten des Unternehmens.

Da das Unternehmen grundsätzlich angehalten ist, die nötigen Betriebsmittel selbst zu stellen, kommt ein verpflichtender BYOD-Einsatz durch Weisung des Arbeitgebers nicht in Frage[35]. Das Direktionsrecht erfasst das Privateigentum der Beschäftigten insoweit nicht[36]. Entscheidet sich das Unternehmen hingegen zur Einführung von freiwilligem BYOD, muss klargestellt werden, in welchem Umfang das Endgerät während der Arbeitszeit für private Zwecke verwendet werden darf.

25 So auch Arning/Moos/Becker, CR 2012, 592, 596.

26 Zum Ganzen Arning/Moos/Becker, CR 2012, 592; Göpfert/Wilke, NZA 2012, 765, 767.

27 Eingehend zu MDM-Lösungen BITKOM (Fn. 22), BYOD 2013, S. 27 ff.; Hemker, DuD 2012, 165, 166 ff.

28 Conrad/Schneider, ZD 2011, 153, 155.

29 Conrad/Schneider, ZD 2011, 153, 155; Kremer/Sander, ITRB 2012, 277; Koch, ITRB 2012, 35, 37.

30 Conrad/Schneider, ZD 2011, 153, 155.

31 Conrad/Schneider, ZD 2011, 153, 155.

32 Göpfert/Wilke, NZA 2012, 765, 766.

33 Arning/Moos/Becker, CR 2012, 592, 594; Göpfert/Wilke, NZA 2012, 765, 766.

34 Zöll/Kielkowski, BB 2012, 2625.

35 Koch, ITRB 2012, 35, 36; Zöll/Kielkowski, BB 2012, 2625.

36 Koch, ITRB 2012, 35, 36; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 23.

Hier ist auf die üblichen arbeitsrechtlichen Maßstäbe zur Online-Nutzung am Arbeitsplatz abzustellen. Ein allzu rigides Management dürfte die Begeisterung der Mitarbeiter für BYOD schwinden lassen. Bei der Ausgestaltung ist zudem ein Reglement zu treffen, wie die Herausgabe der Unternehmensdaten bei Beendigung des BYOD-Programmes bzw. des Beschäftigungsverhältnisses (ggf. nach § 667 BGB direkt oder analog) zu erfolgen hat[37].

Dem mancherorts zu beobachtenden BYOD-Wildwuchs ist in jedem Falle Einhalt zu gebieten. So könnte es sein, dass der Mitarbeiter kraft betrieblicher Übung das Recht erwirbt, eigene Geräte benutzen zu dürfen, ohne dass die Unternehmens-IT hierfür in geeigneter Weise Vorkehrungen treffen konnte[38]. Der umgekehrte Fall einer betrieblichen Übung zu Lasten des Arbeitnehmers und der damit verbundenen obligatorischen Bereitstellung privater Endgeräte ist dagegen nicht zu befürchten[39].

2. Betriebliche Mitbestimmung

Die Vereinbarung, private Endgeräte im Unternehmen zu nutzen, ist ein mitbestimmungspflichtiger Tatbestand. § 87 I BetrVG sieht eine Reihe von Mitbestimmungsrechten des Betriebsrates vor. Ähnliche Vorschriften bestehen im Personalvertretungsrecht der Beamten, vgl. etwa § 75 BPersVG. Gemessen an der Relevanz für die Privatwirtschaft und der Zurückhaltung im öffentlichen Sektor wird gemeinhin allein die Mitbestimmung nach BetrVG diskutiert.

a) § 87 I Nr. 1 BetrVG – Ordnung und Verhalten

Die Anweisungen im Rahmen der Datenschutzorganisation können als Regelungen zum Verhalten der Arbeitnehmer gewertet werden[40]. So verhält es sich etwa bei Anordnungen zur Passwortverwaltung, Malwareschutz oder Updates.

b) § 87 I Nrn. 2 und 3 BetrVG – Arbeitszeit

Geräte mit always-on-Connectivity und die daraus resultierende ständige Erreichbarkeit des Beschäftigten kann Einfluss auf Beginn und Ende der täglichen bzw. betriebsüblichen Arbeitszeit haben[41]. Mit Verwendung privater Consumer-Geräte verwischen die Grenzen zwischen Arbeits- und Freizeitgestaltung zunehmend[42]. Dahingehende Neuregelungen im Unternehmen bedürfen also ebenfalls der Mitwirkung des Betriebsrates.

c) § 87 I Nr. 6 BetrVG – Überwachungsmaßnahmen

Das Protokollieren von Logins, Synchronisationsvorgängen, GPS-Lokalisationsdaten ermöglicht eine nahezu lückenlose Überwachung der Arbeitnehmer[43]. Die datenschutzrechtlichen Kontrollbefugnisse tun ihr Übriges[44]. Entgegen dem missverständlichen Wortlaut der Nr. 6 („dazu bestimmt“) greift das Mitbestimmungsrecht bereits dann ein, wenn die Maßnahme bloß zur Überwachung geeignet ist[45]. Eine gezielte Zweckbestimmung durch den Arbeitgeber ist nicht erforderlich.

3. Betriebsvereinbarung

Nach § 77 IV S. 1 BetrVG können verbindliche Vereinbarungen über sämtliche Gegenstände betrieblicher Mitbestimmung getroffen werden. Eventuelle Probleme der AGB-Inhaltskontrolle werden hierdurch abgemildert (§ 310 IV BGB). Eine wirksame Betriebsvereinbarung gilt zugleich als Rechtsvorschrift im Sinne des § 4 I BDSG[46]. Hierin können also datenschutzrechtliche Befugnisse des Arbeitgebers verankert werden, ohne auf eine Einwilligung des Beschäftigten angewiesen zu sein. Die Vereinbarung gilt insofern als das „Mittel der Wahl“ bei fast allen Fragen mobiler Geräte im Unternehmen[47].

Freilich können mittels einer Betriebsvereinbarung allein die Pflichten des Arbeitgebers sowie Pflichten des Arbeitnehmers bei der Interaktion mit der IT-Infrastruktur des Unternehmens festgelegt werden[48]. Aspekte des Privatlebens sind der Regelungsmacht der Betriebsvereinbarung entzogen. Dazu gehören insbesondere auch Vorschriften über den Abschluss von Reparatur-, Wartungs- und Garantieverträgen, Software- und Hardwareanschaffungen. Auf eine individualvertragliche Regelung kann folglich nicht verzichtet werden.

4. Kosten für Anschaffung und Wartung

Da der Arbeitgeber eigentlich verpflichtet ist, die notwendigen Betriebsmittel selbst zu stellen, stellt sich die Frage, inwiefern die arbeitnehmerseitigen Aufwendungen für BYOD kompensiert werden müssen. So ist

37 Arning/Moos/Becker, CR 2012, 592, 595.

38 Arning/Moos/Becker, CR 2012, 592; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 23; Zöll/Kielkowski, BB 2012, 2625, 2626.

39 Anders wohl Koch, ITRB 2012, 35, 37.

40 Arning/Moos/Becker, CR 2012, 592, 593; Imping/Pohle, K&R 2012, 470, 474 f.; Zöll/Kielkowski, BB 2012, 2625, 2629.

41 Arning/Moos/Becker, CR 2012, 592, 593; Imping/Pohle, K&R 2012, 470, 474 f.; Zöll/Kielkowski, BB 2012, 2625, 2629.

42 Conrad/Schneider, ZD 2011, 153, 156; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 24.

43 Arning/Moos/Becker, CR 2012, 592, 593; Göpfert/Wilke, NZA 2012, 765, 769 f.; Imping/Pohle, K&R 2012, 470, 474 f.; Koch, ITRB 2012, 35, 39; Kremer/Sander, ITRB 2012, 275, 280; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 23.

44 Conrad/Schneider, ZD 2011, 153, 157.

45 Arning/Moos/Becker, CR 2012, 592, 593; Koch, ITRB 2012, 35, 39; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 23.

46 Zum Ganzen Göpfert/Wilke, NZA 2012, 765, 770.

47 Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 23.

48 Conrad/Schneider, ZD 2011, 153, 158.

denkbar, dass sich das Unternehmen anteilig an den Kosten für Anschaffung und Wartung beteiligt[49]. Der Arbeitgeberanteil kann dabei als pauschale Vergütung oder anhand von Einzelnachweisen erfolgen[50].

5. Arbeitnehmerhaftung

Ferner bleibt zu klären, wie bei Verlust oder Beschädigung des privaten Geräts zu verfahren ist. Da BYOD nicht zur Umgehung des Betriebsrisikos dienen soll[51], ist der Arbeitgeber im Zweifel zur Zahlung eines Aufwendungsersatzes verpflichtet (§§ 670, 675 BGB). Ein vertraglicher Pauschalausschluss dieser Ersatzpflicht dürfte AGB-rechtswidrig sein[52]. Der Aufwendungsersatz kann allenfalls dann verweigert werden, wenn die Vergütung im Rahmen der Anschaffung des Gerätes bereits das Schadensrisiko abdecken sollte[53]. Es bedarf hierzu einer klaren Abrede zwischen den Vertragsparteien. Die Betriebshaftpflichtversicherung wird mitarbeitereigene Hardware in der Regel nicht abdecken[54]. Eine gesonderte Geräteversicherung ist deshalb anzuraten[55].

Verletzt der Arbeitnehmer schuldhaft seine Sorgfaltspflichten und trägt dadurch zu einem Datenverlust bei, finden wie gewohnt die Grundsätze der gestuften Arbeitnehmerhaftung Anwendung[56]. Danach haftet der Arbeitnehmer allein bei Vorsatz und grober Fahrlässigkeit in vollem Umfang, bei einfacher Fahrlässigkeit nurmehr anteilig und bei leichter Fahrlässigkeit überhaupt nicht.

V. Lizenzrecht

Softwarehersteller räumen ihren Kunden Nutzungslizenzen an proprietären Produkten ein. Die Software auf mitarbeitereigener Hardware kann unterdessen sowohl vom Beschäftigten als auch vom Unternehmen angeschafft worden sein. Beide müssen diesbezüglich gezielt darauf achten, wie die Lizenzbestimmungen konkret ausgestaltet sind. So wird häufig zwischen privaten und gewerblichen Nutzungsbefugnissen unterschieden. Lizenzen können ferner personen- oder gerätegebunden erteilt werden. Zudem gibt es Mehrplatzlizenzen, oder es besteht die Möglichkeit, ein Softwarepaket sowohl auf einem standortfesten sowie einem mobilen Gerät zu installieren[57].

Consumer-Geräte, insbesondere Notebooks und Tablets werden häufig mit vorinstallierten Betriebssystemen und weiteren Softwarepaketen ausgeliefert, die nicht für den gewerblichen Gebrauch freigegeben sind. Nutzt der Mitarbeiter diese Software dennoch für seinen Beruf, handelt er urheberrechtswidrig. Von genuin urheberrechtswidrig erstellten Kopien ohne jede Art von Lizenz ist hier ganz zu schweigen.

Diese Überlegungen betreffen nicht lediglich den einzelnen Arbeitnehmer, sie gehen auch das Unternehmen an. Denn gemäß § 99 UrhG haftet der Arbeitgeber verschuldensunabhängig für Urheberrechtsverstöße seiner Mitarbeiter[58]. Eine gezielte Bestandsaufnahme und regelmäßige Lizenzaudits sind daher angezeigt, um eventuelle Haftungsrisiken zu minimieren. Zugleich ist zu prüfen, ob sich ggf. Open-Source-lizenzierte Software für die beabsichtigte Verwendung eignet.

VI. Dokumentationspflichten

Im Handels- und Steuerrecht sowie einigen Berufsrechten existieren Vorschriften zur Aufbewahrung von Geschäftsunterlagen[59]. Die entsprechenden Aufbewahrungsfristen betragen in der Regel sechs oder zehn Jahre. Selbstredend kann seitens des Unternehmens nur dokumentiert werden, was auch als Datensatz vorliegt. Conrad und Schneider skizzieren den Fall, dass ein Vertriebsmitarbeiter auf seinem Consumer-Gerät ein Angebot erstellt, dieses mittels seines privaten eMail-Accounts versendet und die Bestätigung an die private Adresse erfolgt[60]. In dieser Situation ist eine Archivierung durch das Unternehmen kaum möglich. Freilich ist einer solchen Vermischung von privaten und geschäftlichen Daten bereits auf Ebene der technisch-organisatorischen Maßnahmen zu begegnen[61]. Bei Verwendung des betrieblichen eMail-Accounts muss hingegen auf eine revisionssichere Archivierung und regelmäßige Synchronisation der Datenbestände hingewirkt werden[62].

VII. Steuerrecht

Gemäß § 3 Nr. 45 EStG sind die Vorteile des Arbeitnehmers aus der privaten Nutzung von betrieblichen

49 Zöll/Kielkowski, BB 2012, 2625, 2626.

50 Arning/Moos/Becker, CR 2012, 592, 593.

51 Imping/Pohle, K&R 2012, 470, 472 zum allgemeinen Rechtsgedanken des § 615 S. 3 BGB.

52 Göpfert/Wilke, NZA 2012, 765, 769.

53 Arning/Moos/Becker, CR 2012, 592, 597; Walter/Dorschel, Wirtschaftsinformatik & Management 2012, 22, 25 f.; Zöll/Kielkowski, BB 2012, 2625, 2627.

54 Conrad/Schneider, ZD 2011, 153, 158.

55 Zöll/Kielkowski, BB 2012, 2625, 2628.

56 Göpfert/Wilke, NZA 2012, 765, 769; Zöll/Kielkowski, BB 2012, 2625, 2627.

57 Zu den einzelnen Spielarten Conrad/Schneider, ZD 2011, 153, 157.

58 Arning/Moos/Becker, CR 2012, 592, 597; Göpfert/Wilke, NZA 2012, 765, 767; Herrnleben, MMR 2012, 205, 206. Ausführlich zu § 99 UrhG sowie zur parallel gelagerten Organhaftung im Unternehmen jüngst Söbbing/Limbacher, ITRB 2013, 110, 112 f.

59 § 247 HGB (Handels- und Geschäftsbriefe, auch in elektronischer Form), § 147 AO, § 14b UStG, GoBS & GDPdU des BMF, § 10 III MBOÄ u.w.m.

60 Conrad/Schneider, ZD 2011, 153, 158.

61 So bereits Imping/Pohle, K&R 2012, 470, 474.

62 Göpfert/Wilke, NZA 2012, 765, 768; Koch, ITRB 2012, 35, 36.

Datenverarbeitungs- und Telekommunikationsgeräten neuerdings steuerfrei[63]. Der Wortlaut erfasst indes keine Geräte, die sowieso dem Arbeitnehmer gehören, und deren Anschaffung vom Arbeitgeber besonders vergütet wird. Insoweit kommt allenfalls eine Steuerfreiheit für Auslagenersatz nach § 3 Nr. 50 EStG oder ein Abzug für Werbungskosten nach § 9 I S. 2 EStG in Betracht. Aufwendungen, die ausschließlich dem Privatbereich entspringen, dürfen gemäß § 12 Nr. 1 EStG jedoch nicht berücksichtigt werden. Insoweit ist eine genaue arbeitsvertragliche Regelung zur BYOD-Vergütung erforderlich[64]. Umsatzsteuerrechtlich ist BYOD ebenfalls nicht ausdrücklich vom Gesetz erfasst[65]. Der BITKOM-Verband hat in einer Broschüre einige steuerrechtliche Fallbeispiele zusammengestellt[66].

VIII. Strafrecht

Der strafrechtliche Schutz von Berufsgeheimnissen ist in § 203 StGB vorgesehen, derjenige unternehmensbezogener Daten in den §§ 17 ff. UWG. Die fahrlässige Begehung dieser Tatbestände durch fehlerhaften Umgang mit dem Datenverarbeitungsgerät ist dabei gemäß § 15 StGB straflos. Gegen die vorsätzliche Verwirklichung ist unterdessen kein IT-sicherheitstechnisches Kraut gewachsen[67], so dass auf die Lenkungswirkung des Strafrechts vertraut werden muss.

Die spezifisch computerstrafrechtlichen Delikte[68] wie das Ausspähen von Daten nach § 202a I StGB oder die Datenveränderung nach § 303a I StGB sind bei Betrachtung der Arbeitgeberseite interessant, dürften aber bei konsequenter Trennung von privaten und unternehmensbezogenen Daten eigentlich keine Rolle spielen. Dateizugriffe via Mobile Device Management sollten die mitarbeitereigenen Daten schlichtweg ausklammern. Hinsichtlich der unternehmensbezogenen Daten wird es an der Rechtswidrigkeit des Zugriffs fehlen, wenn Daten ausgelesen oder verändert werden. Ob die Daten überhaupt tatbestandsmäßig im Sinne des § 202a I StGB gegen unberechtigten Zugang besonders gesichert sind, kann nur einzelfallabhängig beurteilt werden. Sicherungseinrichtungen von Fernadministrationsschnittstellen im Mobile Device Management sind jedenfalls zwangsläufig solche des Unternehmens und nicht des einzelnen Users[69].

Problematisch wird es, wenn wegen Verlusts oder Diebstahls des Gerätes ein Remote-Wipe initialisiert werden soll.[70] Dabei werden regelmäßig alle Daten auf dem Gerät gelöscht oder unbrauchbar gemacht. § 303a I StGB erfordert keine besondere Sicherung der Daten. Die Einwilligung zur Vernichtung privater Daten kann im Vorhinein eingeholt werden und stellt ein tatbestandsausschließendes Einverständnis dar[71]. Mit einer solchen Einwilligung ist unterdessen wenig gewonnen, wenn mit der Verlustanzeige an das Unternehmen zugleich ein Widerruf der Löschbewilligung erfolgt. Zur Absicherung aller Unwägbarkeiten ist also eine feingranulare MDM-Lösung erforderlich, die in der Lage ist, Daten selektiv zu löschen.

IX. Alternativen

1. Choose your own device (CYOD)

Der Arbeitgeber hat natürlich auch die Möglichkeit, die einzusetzenden Endgeräte selbst anzuschaffen. Dies grenzt die Zahl der möglichen Hard- und Softwarekombinationen und damit den Administrationsaufwand auf Seiten der IT-Abteilung erheblich ein[72]. Zugleich kann ein einheitliches MDM sichergestellt werden[73]. Mengenrabatte im Einkauf und beim Abschluss von Wartungsverträgen dürften die Folge sein. Da die Geräte im Eigentum des Unternehmens stehen, können die Nutzungsvorgaben weitgehend frei bestimmt werden. Auch ist zu erwarten, dass Mitarbeiter die mit den datenschutzrechtlichen Vorgaben verbundenen Einschränkungen eher hinnehmen werden, wenn es sich um unternehmenseigene Hardware handelt.

2. Mitarbeiter-PC-Programm (MPP)

Daneben existiert das von der Bundesregierung unterstützte Mitarbeiter-PC-Programm der Initiative D21[74]. Im Zuge des Programms schafft der Arbeitgeber die Geräte an, welche dann zwecks privater und dienstlicher Nutzung von den Mitarbeitern geleast werden. Dieses Vorgehen ist steuerlich vergünstigt. Zugleich kann sich das Unternehmen die Vorteile von CYOD zunutze machen.

63 BITKOM (Fn. 22), BYOD 2013, S. 12.

64 Im Ergebnis auch BITKOM (Fn. 22), BYOD 2013, S. 13.

65 BITKOM (Fn. 22), BYOD 2013, S. 12 f. zu § 3 IXa UStG.

66 BITKOM (Fn. 22), BYOD 2013, S. 13-16.

67 Optimistischer insoweit Imping/Pohle, K&R 2012, 470, 474.

68 Hierzu näher Söbbing/Müller, ITRB 2011, 263 ff. und jüngst Söbbing, RDV 2013, 77 ff.

69 Sie geben als solche kein besonderes Geheimhaltungsinteresse des Beschäftigten zu erkennen.

70 Die private Verwendung dienstlicher eMail-Accounts erzeugt indes keine besonderen Probleme, da der eMail-Verkehr in der Regel über Unternehmensserver abgewickelt wird. Der singuläre eMail-Abruf etwa via POP3 allein auf das jeweilige Gerät ist im Unternehmensumfeld nur schwer vorstellbar.

71 Arning/Moos/Becker, CR 2012, 592, 596.

72 Imping/Pohle, K&R 2012, 470, 476.

73 Koch, ITRB 2012, 35, 39. In diesem Sinne bereits BITKOM (Fn. 22), BYOD 2013, S. 24 und BSI (Fn. 14), Consumerization 2013, S. 7.

74 Einzelheiten unter www.initiatived21.de/portfolio/mpp, näher Hörl, ITRB 2012, 258 ff.

X. Fazit

Die Einführung von BYOD im Unternehmen kann nur das Ergebnis einer umfassenden Analyse rechtlicher und IT-spezifischer Risiken sein. Die Risikobewertung kann dabei nicht sinnvollerweise losgelöst von konkreten Hard- und Softwarekombinationen erfolgen. IT-, Datenschutz- und ggf. die Rechtsabteilung müssen hier zweckmäßig zusammenwirken.

Eine konsequente Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen bedeutet einen gesteigerten Administrationsaufwand und beschneidet die Eigentumsrechte am privaten Gerät in erheblicher Weise[75]. Die zu erwartende Kostenersparnis und die beabsichtigte Steigerung der Mitarbeiterzufriedenheit können sich somit schnell als Fehleinschätzung darstellen. Deswegen sind alternative Konzepte wie CYOD und MPP bei der Planung stets zu berücksichtigen.

Dem eigenmächtigen Wildwuchs und der sog. „Schatten-IT" sind indes durch eindeutige Regelungen, ggf. dem Totalverbot, Einhalt zu gebieten. Kann ein angemessenes Datenschutzniveau nicht gewährleistet werden, ist auf den Einsatz von BYOD wohl oder übel komplett zu verzichten. ■

75 BITKOM (Fn. 22), BYOD 2013, S. 33; Zöll/Kielkowski, BB 2012, 2625.