leichter ist, bei Bedarf kritische Kontakte mit potentiellen „Mittätern" durch entsprechende Pauschalverbote zu minimieren.

Auch bei der Entwicklung globaler Compliance-Programme dürften im vertikalen Bereich lokale Besonderheiten etwas stärker zu berücksichtigen sein, als im horizontalen Bereich. Sobald ein „rule of reason"-Ansatz wie bspw. in den USA zu berücksichtigen ist, wird die Compliance-Beratung noch komplexer.

III. Reaktionsmöglichkeit bei Feststellung eines Verstoßes?

Wird trotz aller Compliance-Maßnahmen im Rahmen einer internen Untersuchung ein Verstoß festgestellt, stellt sich häufig mangels entsprechender Programme der Kartellbehörden zwar nicht die Frage nach einem echten Kronzeugenantrag. Gleichwohl kann insbesondere angesichts der gewährten Bußgeldreduktionen im Falle der Kooperation mit den Behörden (vor allem auch aufgrund der jüngsten Entscheidungen der EU-Kommission) überlegt werden, die Behörden über den Verstoß zu informieren und auf Bußgeldreduktion zu hoffen. Während aber bei einem horizontalen Fall die Wettbewerber unter sämtlichen Nachteilen einer behördlichen Ermittlung leiden und einem Bußgeldrisiko ausgesetzt werden, sind bei einer Selbstanzeige durch den Hersteller in vertikalen Fällen die eigenen Kunden (= Händler) massiv betroffen. Diese Beziehungen dürften bei einer Selbstanzeige auf Jahre beschädigt sein. Daher gilt wie so oft auch hier: Wehret den Anfängen!

KONTAKT:

Dr. Johannes Dittrich
Linde AG
Klosterhofstraße 1
80331 München
Tel.: 089/35757 1493
johannes.dittrich@linde.com

RECHTSANWÄLTE DR. STEFAN BARTZ UND DR. MARCO GROTENRATH*

„Bring Your Own Device"-Geräte in internen Ermittlungen

A. Einleitung

„Bring Your Own Device" (im Folgenden „BYOD") beschreibt die vom Arbeitgeber angebotene Möglichkeit, dass Arbeitnehmer eigene elektronische Geräte wie Laptops, Tablets oder Smartphones auch zu Arbeitszwecken verwenden können. Der Arbeitgeber bindet diese hierzu in die eigene IT-Infrastruktur ein. Begründet wird BYOD unter anderem damit, dass Unternehmen ihren Arbeitnehmern ermöglichen wollen, mit den Geräten zu arbeiten, die sie auch privat nutzen.[1] Zugleich erlaubt BYOD je nach Ausgestaltung, Einkaufs- und Wartungskosten auf den Arbeitnehmer zu verlagern.[2]

Neben einer Vielzahl vor allem arbeitsrechtlicher Fragestellungen[3] wirft BYOD auch bei internen Untersuchungen diverse rechtliche Probleme auf. Grundlage und wichtigstes Mittel zur Informationsgewinnung in nahezu jeder internen Untersuchung ist die Sichtung der Kommunikation der Angestellten.[4] Wenn der Arbeitnehmer nicht unternehmenseigene, sondern private Kommunikationsgeräte nutzt, ist zu prüfen, ob und unter welchen Voraussetzungen der Arbeitgeber das BYOD-Gerät bei internen Untersuchungen vom Arbeitnehmer herausverlangen und die darauf befindlichen Daten sichten darf. Die datenschutzrechtlichen Anforderungen und Risiken aufgrund der am 25.5.2018 in Kraft getretenen Datenschutzgrundverordnung (DSGVO) führen dabei zu zusätzlichen Herausforderungen.

B. Rechtliche und technische Grundlagen von BYOD

BYOD kann rechtlich und technisch unterschiedlich ausgestaltet sein. Die Ausgestaltung hat Einfluss auf die Rechte und Pflichten der Parteien und wirkt sich unmittelbar auf die Sichtungsmöglichkeiten bei internen Untersuchungen aus. Unternehmen sollten daher bei Einführung von BYOD stets berücksichtigen, wie sie dessen Vorteile nutzen und zugleich den Zugriff auf sowie den Erhalt von Geschäftsdaten und -korrespondenz sicherstellen können.

I. Rechtliche Ausgestaltungsmöglichkeiten von BYOD

Bei der rechtlichen Ausgestaltung ist danach zu differenzieren, wer Eigentümer des Endgeräts ist, wem also Ausschluss- und Abwehrrechte gegen fremde Zugriffe (§ 903 BGB) zustehen. Die Einzelheiten der jeweiligen Rechte und Pflichten sowie der Zugriffsmöglichkeiten auf Gerät und Daten sind im Idealfall vertraglich zwischen Arbeitgeber und -nehmer geregelt.

Bei dem sog. *„Personally-Owned-Company-Enabled"*-Modell (im Folgenden „POCE-Modell") erwirbt der Arbeitnehmer selbst Eigentum am Gerät.[5] Hierfür erhält er

* Dr. Stefan Bartz ist Senior Associate und Dr. Marco Grotenrath Associate im Hamburger Büro der Kanzlei Latham & Watkins LLP; sie sind Mitglieder der White Collar Defense & Investigations Practice Group.

1 Vgl. Kramer/*Solmecke*, IT-Arbeitsrecht, 2017, Kap. B, Rn. 17; Kramer/*Hoppe*, IT-Arbeitsrecht, 2017, Rn. 616.

2 *Göpfert/Wilke* NZA 2012, 765.

3 Vgl. hierzu zB *Göpfert/Wilke* NZA 2012, 765 ff.; *Pollert* NZA-Beilage 2014, 152 ff.; *Wulf/Burgenmeister* CB 2014, 374 ff.; *Lipp* DSRITB 2013, 747 ff.; *Buchholz* DSRITB 2012, 841 ff.

4 Zu möglichen Mitteln der Sachverhaltsaufklärung bei internen Investigationen vgl. *Mengel/Ullrich* NZA 2006, 240 (241 ff.).

5 Vgl. *Imping/Pohle* K&R 2012, 470 (471); *Monsch*, Bring Your Own Device (BYOD), 2017, S. 25.

zumeist einen Pauschalbetrag vom Unternehmen.[6] Das Unternehmen ermöglicht dem Arbeitnehmer sodann, das Gerät in die eigene Systemumgebung einzubringen, indem etwa der Zugriff auf Unternehmensserver und -software gestattet wird. Im Gegenzug räumt der Arbeitnehmer dem Unternehmen (Fern-)Zugriff auf das Gerät ein. Beim *„Corporate-Owned-Personally-Enabled"*-Modell (im Folgenden „COPE-Modell")[7] erwirbt das Unternehmen das Endgerät und bleibt dessen Eigentümer. Dem Arbeitnehmer wird ausdrücklich die private Nutzung des Geräts für die Dauer des Dienstverhältnisses gestattet.

Die nachfolgenden Ausführungen beziehen sich in erster Linie auf das POCE-Modell, da insbesondere hierbei die besonderen rechtlichen Probleme und Fragestellungen im Zuge interner Ermittlungen entstehen.

II. Technische Ausgestaltungsmöglichkeiten von BYOD

Bei BYOD lagert das Unternehmen Teile der eigenen IT-Infrastruktur an eine Privatperson aus,[8] möchte aber – idealerweise jederzeitigen – Zugriff auf die Daten behalten, die der Arbeitnehmer im Rahmen seiner dienstlichen Tätigkeit erlangt oder produziert.[9] Die Eingriffs- und Kontrollmöglichkeiten des Arbeitgebers finden jedoch in der grundrechtlich geschützten Privatsphäre des Arbeitnehmers (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) ihre Schranken. Unternehmen sollten daher versuchen, private und dienstliche Daten auf dem Endgerät durch eine geeignete technische Ausgestaltung von BYOD möglichst strikt voneinander zu trennen.[10]

Eine bewährte Methode für die danach notwendige Datentrennung ist das sog. *„Closed Containering"* oder auch *„Sandboxing"*.[11] Dabei wird auf dem Speicher des Geräts ein virtueller „Raum" abgeschottet und mit einer Verschlüsselung und einem Passwort gesichert. Hierin lagert die Software sensible Firmendaten. Der Arbeitnehmer muss jeweils entscheiden, ob er innerhalb des geschlossenen dienstlichen Bereichs oder auf seinem privaten Benutzerkonto arbeiten möchte und kann so eine Trennung privater und dienstlicher Daten ermöglichen. Alternativ verbleiben die Daten beim Unternehmen und der Arbeitnehmer greift über sein eigenes Gerät nur aus der Ferne auf diese zu. Bei dieser sog. *„Virtualisierungslösung"* wird auf dem Endgerät ein Programm virtuell dargestellt; eine dauerhafte Speicherung der Daten des Arbeitnehmers erfolgt ausschließlich auf dem Unternehmensserver.[12]

Eine strikte Trennung dienstlicher und privater Daten setzt indes nicht nur eine technische Lösung voraus, sie funktioniert nur, wenn Arbeitnehmer die Trennung auch beachten. Hinzu kommt, dass dienstliche Kommunikation nicht mehr nur auf vom Unternehmen bereitgestellten Kommunikationskanälen (E-Mail, Messenger) erfolgt, sondern Arbeitnehmer hierfür auch auf Drittanbieter wie *WhatsApp* oder *iMessage* ausweichen.[13] Das Unternehmen kann diese Kommunikationskanäle nicht überwachen. Daher ist eine Anweisung ratsam, dass dienstliche Kommunikation ausschließlich über vom Arbeitgeber bereitgestellte Wege zu erfolgen hat.[14] Die Nutzung entsprechender Dienste auf dem privaten BYOD-Gerät grundsätzlich zu untersagen, würde das Konzept von BYOD jedoch *ad absurdum* führen.[15]

Selbst bei entsprechender Weisung zur Trennung privater und dienstlicher Kommunikation dürfte dies auch gewillte Arbeitnehmer vor faktische Probleme stellen. Eine Unterscheidung zwischen dienstlichem und privatem Inhalt ist nicht immer möglich und die Grenzen sind fließend.[16] Eine technische Lösung für dieses Problem existiert bislang nicht und ist auch schwer vorstellbar, da sich eine einheitliche Kommunikation nicht künstlich aufspalten lässt. Es ist daher Aufgabe des Arbeitnehmers, die Kommunikation zu steuern und dienstliche und private Inhalte im eigenen Interesse möglichst frühzeitig zu trennen.

C. BYOD in internen Ermittlungen im Unternehmen

Besteht der Verdacht einer unternehmensbezogenen Straftat oder eines Compliance-Verstoßes, ist es die Pflicht und im Interesse des betroffenen Unternehmens, den Sachverhalt aufzuklären,[17] um materielle und immaterielle Schäden zu vermeiden.[18] Dies geschieht vor allem durch interne Ermittlungen.

I. Interne Ermittlungen als Instrument zur Sachverhaltsaufklärung

Interne Ermittlungen dienen zum einen dazu, behördlichen Verfahren zuvorzukommen[19] oder diese kooperativ zu begleiten. Zum anderen sind sie integraler Bestandteil eines effektiven Compliance-Management-Systems.[20] Bei transatlantischen Sachverhalten mit Beteiligung von US-Behörden können Unternehmen bei umfassender Kooperation ferner auf Strafmaß- bzw. Bußgelderleichterungen hoffen. Deutsche Behörden sind bei der Berücksichtigung von Kooperation und (grundsätzlich) wirksamen Compliance-Systemen bislang noch zurückhaltend.[21] Ob sich dies durch

---

6 Etwaige Zusatzkosten, die daraus resultieren, dass der Arbeitnehmer ein teureres Gerät wählt, muss er in der Regel selbst tragen.

7 Wie „POCE" entstammt auch der Begriff „COPE" dem US-amerikanischen Sprachraum; u. a. auch verwendet in Hauschka/Moosmayer/Lösler/*Schmid*, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 216 ff.; *Monsch*, Bring Your Own Device (BYOD), 2017, S. 25 ff.

8 *Conrad/Schneider* ZD 2011, 153 ff.

9 Dies gilt für die Zeit während des Arbeitsverhältnisses, aber auch für die Zeit danach, vgl. *Buchholz* DSRITB 2012, 841 (843). Unabhängig davon, auf welchem Gerät Inhalte produziert werden, treffen das Unternehmen unter Umständen Aufbewahrungspflichten, § 257 HGB.

10 So auch *Koch* ITRB 2012, 35 (37); *Imping/Pohle* K&R 2012, 470 (471); *Göpfert/Wilke* NZA 2012, 765 (766).

11 So der Begriff bei *Buchholz* DSRITB 2012, 841 (843).

12 *Bierekoven* ITRB 2012, 106 (107); *Imping/Pohle* K&R 2012, 470 f.

13 *Schrey/Kielkowski/Gola* MMR 2017, 656 f.

14 Zu Risiken, welche die Nutzung privater Geräte zu dienstlichen Zwecken mit sich bringen kann, vgl. *Koch* ITRB 2012, 35 (36 f.).

15 So *Koch* ITRB 2012, 35 f.

16 Vgl. *Bierekoven* ITRB 2012, 106 (107); *Ernst* NZA 2002, 585 (588).

17 LG München I 10.12.2013 – 5 HK O 1387/10 = CCZ 2014, 142; *Wybitul* NJW 2014, 3605 (3606).

18 Es besteht eine Legalitäts- und Aufklärungspflicht der Unternehmensführung, vgl. zB § 91 Abs. 2 AktG, §§ 30, 130 OWiG; vgl. auch *Wybitul* NJW 2014, 3605 (3606); aA jedenfalls für interne Ermittlungen außerhalb des Finanzsektors Knierim/Rübenstahl/Tsambikakis/*Nestler*, Internal Investigations, 2. Aufl. 2016, S. 6 Rn. 13.

19 Dies gilt insbesondere in Bezug auf die Kronzeugenregelung im Kartellrecht, vgl. etwa *Wettner/Mann* DStR 2014, 655 ff.

20 IDW PS 980 (69. Erg.-Lfg. Feb. 2019) Ziff. 5.4.3.1.

21 Vgl. BGH NJW 2017, 3798, wonach sich ein effizientes Compliance-Management-Systems bußgeldmindernd auswirken kann; *Eufinger* CCZ 2016, 209 ff.

das geplante Verbandssanktionengesetz ändern wird, bleibt abzuwarten. Daneben können interne Ermittlungen auch der Prüfung und Sicherung von Schadensersatzansprüchen und arbeitsrechtlichen Maßnahmen gegenüber beteiligten Personen dienen.[22]

Kern der Sachverhaltsaufklärung ist regelmäßig die Befragung von möglicherweise beteiligten Arbeitnehmern sowie die Sichtung der mit dem potentiellen Fehlverhalten in Verbindung stehenden Kommunikation.[23] Unternehmensinterne Ermittlungen bewegen sich daher stets im Spannungsfeld zwischen dem Aufklärungsinteresse des Arbeitgebers und dem Interesse des Arbeitnehmers an Geheimhaltung und Schutz seiner Daten sowie der Vertraulichkeit seiner Kommunikation.

Die Debatte um die Reichweite der Befugnisse des Arbeitgebers bei internen Ermittlungen bekommt bei BYOD aufgrund der rechtlichen Beziehung des Arbeitnehmers zum Endgerät eine zusätzliche Dimension. Denn im Gegensatz zu herkömmlichen IT-Durchsuchungen von Arbeitsmitteln muss der Arbeitgeber das mobile BYOD-Endgerät in einem ersten Schritt vom Arbeitnehmer herausverlangen, soweit sich die Daten nicht auf einem Unternehmensserver befinden oder per Fernzugriff verfügbar sind. Sofern das Unternehmen keine strikte Cloud-Lösung nutzt, lässt es sich jedenfalls nie ausschließen, dass Daten auch lokal auf dem Endgerät gespeichert werden. Erst im zweiten Schritt stellt sich die Frage, ob und wie die sich auf dem Gerät befindlichen Daten des Arbeitgebers gesichtet werden dürfen und inwieweit BYOD hierauf Einfluss hat.

II. Die Besitzstellung bei BYOD-Geräten

Stellt der Arbeitgeber dem Arbeitnehmer betriebliche Arbeitsmittel zu Verfügung, ist dieser in Bezug auf die Arbeitsmittel weisungsgebunden und damit nur als Besitzdiener des Arbeitgebers anzusehen.[24] Die Weisungsgebundenheit findet insbesondere in der jederzeitigen Zugriffsmöglichkeit des Besitzherrn auf die Sache Ausdruck.[25]

Werden betriebliche Arbeitsmittel nicht vom Arbeitgeber überlassen, sondern findet zwischen Arbeitgeber und Arbeitnehmer eine BYOD-Vereinbarung nach dem POCE-Modell Anwendung, besteht indes keine jederzeitige Zugriffsmöglichkeit des Arbeitgebers auf das Gerät. Die Vereinbarung billigt dem Arbeitnehmer als Eigentümer vielmehr weitgehend eigenständige Nutzungsbefugnisse zu. Selbst während der Arbeitszeit kann der Arbeitgeber typischerweise nicht bestimmen, auf welche Weise der Arbeitnehmer mit dem Endgerät verfahren soll. Er ist im Hinblick auf die Nutzung des Geräts (wenn überhaupt) nur partiell weisungsbefugt. Der Arbeitnehmer kann sich – vorbehaltlich besonderer vertraglicher Regelungen – als Eigentümer und Besitzer gegen einen unberechtigten Entzug des Geräts durch den Arbeitgeber zur Wehr setzen (§§ 861, 858 BGB).

22 *Schrader/Mahler* NZA-RR 2016, 57.
23 Zu diesen und weiteren Möglichkeiten interner Ermittlungen durch den Arbeitgeber vgl. *Schrader/Mahler* NZA-RR 2016, 57 (58 ff.).
24 Zur Besitzdienerschaft des Arbeitnehmers in Bezug auf Arbeitsmittel vgl. BAG 17.9.1998 – 8 AZR 175/97 = NJW 1999, 1049; auch LAG Berlin 26.5.1986 – 9 Sa 24/86 = NJW 1986, 2528; Ring/Grziwotz/Keukenschrijver/*Hoeren*, BGB Sachenrecht, 4. Aufl. 2016, § 855 Rn. 10.
25 Vgl. BeckOGK BGB/*Götz*, Stand 1.4.2019, § 855 Rn. 14; Ring/Grziwotz/Keukenschrijver/*Hoeren*, BGB Sachenrecht, 4. Aufl. 2016, § 855 Rn. 6.

III. Herausgabeanspruch des Arbeitgebers in Bezug auf das BYOD-Gerät

Hat der Arbeitgeber keine Möglichkeit, die Daten auf dem BYOD-Gerät per Fernzugriff zu sichten, muss er dieses zunächst vom Arbeitnehmer herausverlangen. Dem Arbeitgeber können insoweit vertragliche sowie gesetzliche Herausgabeansprüche zustehen.

1. Vertragliche Herausgabeansprüche

Die Parteien können im oder als Zusatz zum Arbeitsvertrag eine Herausgabeklausel für den Fall interner Durchsuchungen explizit vereinbaren.[26] Hierbei sollten die Fälle, in denen eine Pflicht zur Herausgabe des Geräts besteht, individualvertraglich genau spezifiziert sein. Dem Arbeitnehmer muss es möglich sein, im Einzelfall vorherzusehen, unter welchen Umständen er mit der Herausgabe rechnen muss, etwa bei einem konkreten Verdacht einer unternehmensbezogenen Straftat oder eines Compliance-Verstoßes. Eine Herausgabeklausel, die vom Arbeitgeber mit einer Vielzahl von Arbeitnehmern abgeschlossen wird, unterliegt als Allgemeine Geschäftsbedingung zudem einer Inhaltskontrolle nach § 307 Abs. 1 BGB und darf den Arbeitnehmer nicht entgegen Treu und Glauben unangemessen benachteiligen.[27]

Herausgabeansprüche in Fällen interner Untersuchungen kommen jedoch auch in Betracht, wenn lediglich eine abstrakte BYOD-Vereinbarung zwischen Arbeitgeber und Arbeitnehmer existiert und ausdrückliche Regelungen zu Herausgabepflichten fehlen. Sieht man BYOD-Absprachen als Geschäftsbesorgungs-[28] bzw. Mietvertrag[29] in Bezug auf das Endgerät an, lassen sich Herausgabepflichten des Arbeitnehmers nach den jeweiligen gesetzlichen Regelungen[30] sowie durch ergänzende Auslegung der beidseitigen Parteiinteressen konstruieren.[31] Jedoch dürfen solche Herausgabeansprüche inhaltlich nicht weiter reichen als zulässige vertragliche Ansprüche. Danach kommen insbesondere anlasslose Herausgabepflichten des Arbeitnehmers nicht in Betracht. Es ist jedenfalls ein auf Tatsachen gestützter konkreter Verdacht eines Compliance-Verstoßes zu fordern.

Weiter ist eine arbeitsvertragliche Nebenpflicht (§§ 611, 241 Abs. 2 BGB) zur Herausgabe des BYOD-Geräts denkbar, um Schäden vom Arbeitgeber abzuwenden.[32] Ein sol-

26 Eine einseitige Weisung des Arbeitgebers zur Implementierung von BYOD gegenüber dem Arbeitnehmer ist dagegen nicht möglich, da die betriebsmittelersetzende Nutzung eigener Geräte nicht mehr vom Direktionsrecht des Arbeitgebers gedeckt ist, *Seel* MDR 2014, 69 (70).
27 Auer-Reinsdorff/Conrad/*Conrad*, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 37 Rn. 290; *Göpfert/Wilke* NZA 2012, 765 (769); *Monsch*, Bring Your Own Device (BYOD), 2017, S. 95; *Seel* MDR 2014, 69 (70).
28 Vgl. etwa *Imping/Pohle* K&R 2012, 470 (471); grundsätzlich hierzu *Koch* ITRB 2012, 35 (37).
29 Vgl. *Koch* ITRB 2012, 35 (37). Vorliegend wird unterstellt, dass der Arbeitnehmer – wie üblich – für die Bereitstellung seines Geräts eine Art finanzieller Kompensation erhält, weshalb keine bloße Leihe oder ein Auftrag angenommen werden.
30 § 535 Abs. 1 S. 1 BGB bzw. §§ 675 Abs. 1, 667 BGB.
31 Grundsätzlich gegen einen Rückgriff auf neben arbeitsvertraglichen Regelungen bestehende Herausgabeansprüche *Monsch*, Bring Your Own Device (BYOD), 2017, S. 31 ff.; *Zöll/Kielkowski* BB 2012, 2625 (2626); *Wulf/Burgenmeister* CB 2014, 374 (377); anders *Göpfert/Wilke* NZA 2012, 765 (769); *Imping/Pohle* K&R 2012, 470 (471).
32 Vgl. nur BAG 16.2.1995 – 8 AZR 493/93 = NZA 1995, 565; BAG 9.9.2015 – 7 AZR 668/13 = NZA 2016, 435; ausführl. Erfurter Kommentar zum Arbeitsrecht/*Preis*, 19. Aufl. 2019, § 611a Rn. 744 ff.

cher Herausgabeanspruch dürfte nur in Ausnahmen in Betracht kommen, wenn die besonderen Umstände des Einzelfalles und die überwiegenden Interessen des Arbeitgebers dies rechtfertigen. Für eine Herausgabepflicht kann etwa der Verdachtsgrad, die Höhe des drohenden Schadens, die Erforderlichkeit der Sichtung der Daten für die Aufklärung des Sachverhaltes und die Dauer der Entziehung des Geräts sprechen.[33] Auch hier gilt, dass der Anspruch nicht weitergehen darf als entsprechende vertragliche Regelungen, um ausdrückliche Abreden zu BYOD nicht zu unterlaufen.

Ohne eine ausdrückliche Regelung lassen sich Herausgabepflichten im Ergebnis nur schwer und stets abhängig vom Einzelfall herleiten. Vorzugswürdig im Interesse beidseitiger Rechtssicherheit ist, Inhalt und Umfang von Herausgabeansprüchen für die Fälle interner Ermittlungen explizit vertraglich zu fixieren.[34]

Schließlich ist zu bedenken, dass selbst bei Bestehen eines Herausgabeanspruchs eine gerichtliche Durchsetzung desselben bei Weigerung des Arbeitnehmers selten von Seiten des Unternehmens gewollt sein wird. Die Verfahrensdauer würde das Ziel einer zügigen Durchführung interner Ermittlungen vereiteln. Zudem werden Unternehmen die Öffentlichkeit eines Gerichtsverfahrens im Zusammenhang mit laufenden internen Ermittlungen meiden. Der Arbeitgeber sollte daher stets versuchen, eine einvernehmliche Herausgabe des Geräts zu erreichen.

2. Gesetzliche Herausgabeansprüche

Beim POCE-Modell erwirbt der Arbeitnehmer selbst das Eigentum an dem Gerät. Auch wenn der Mitarbeiter das Gerät im Rahmen betrieblicher Zwecke nutzt, verbleiben das Gerät sowie die auf diesem installierten Kopien des Betriebssystems und der Anwendungssoftware in seinem Eigentum.[35] Ein Vindikationsanspruch des Arbeitgebers kommt damit nicht in Betracht.[36]

IV. Recht des Arbeitgebers auf Auslesen und Sichten der Daten des BYOD-Geräts

Hat der Arbeitgeber das BYOD-Gerät erfolgreich herausverlangt, muss er die sich auf dem Gerät befindlichen dienstlichen Daten des Arbeitnehmers in einem zweiten Schritt auslesen und sichten. Auch hierfür bestehen aufgrund von BYOD rechtliche Besonderheiten.

1. Rechtsgrundlagen für eine Datenverarbeitung im Zuge interner Ermittlungen

Das Auslesen und Sichten von Daten auf einem BYOD-Gerät im Zuge interner Ermittlungen stellt eine Datenverarbeitung des Arbeitgebers dar (Art. 4 Nr. 2 DSGVO). Sie darf nur erfolgen, wenn die betroffene Person wirksam einwilligt oder ein gesetzlicher Erlaubnistatbestand eingreift (sog. „Verbot mit Zulässigkeitstatbeständen").[37] Ergänzend tritt das aus dem allgemeinen Verhältnismäßigkeitsgrundsatz abgeleitete Prinzip der Erforderlichkeit hinzu (Art. 6 Abs. 1 S. 1 lit. f) DSGVO). Aufgrund der potenziell sensiblen Daten auf einem BYOD-Gerät und sofern dem Arbeitnehmer weitreichende Konsequenzen drohen, kann zudem eine Datenschutz-Folgenabschätzung geboten sein (Art. 35 DSGVO).

Der für eine zulässige Datenverarbeitung erforderliche Erlaubnistatbestand kann in einer – möglicherweise bereits arbeitsvertraglich geregelten – Einwilligung des Arbeitnehmers in das Auslesen und Sichten der Daten liegen (§ 26 Abs. 2 BDSG). Allerdings sind die Anforderungen an eine wirksame Einwilligung durch die DSGVO weiter gestiegen. Ferner kommt eine Datenverarbeitung gem. § 26 Abs. 1 S. 1 BDSG zur Aufklärung von Pflichtverletzungen im Beschäftigungsverhältnis sowie nach § 26 Abs. 1 S. 2 BDSG in Betracht, wenn ein konkreter Verdacht einer Straftat besteht.[38] Außerhalb des Beschäftigungsverhältnisses kann zudem auf die Erfüllung rechtlicher Verpflichtungen und die Wahrung der berechtigten Interessen des Arbeitgebers als Verantwortlichen zurückgegriffen werden (Art. 6 Abs. 1 S. 1 lit. c) und f) DSGVO). Schließlich kann eine Betriebsvereinbarung nach Art. 88 DSGVO iVm § 26 Abs. 4 BDSG eine mögliche Rechtsgrundlage der Datenverarbeitung darstellen.[39]

a) Einwilligung in die Datenverarbeitung, § 26 Abs. 2 BDSG

Die Voraussetzungen einer wirksamen Einwilligung nach § 26 Abs. 2 BDSG in die Datenverarbeitung im Beschäftigungsverhältnis sind umstritten.[40] Für das Auslesen und Sichten der Daten von BYOD-Geräten bestehen zusätzliche Bedenken.

Die – jederzeit widerrufliche (Art. 7 Abs. 3 DSGVO) – Einwilligung im Beschäftigungskontext muss freiwillig erfolgen. Dabei sind insbesondere die Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt wurde, zu berücksichtigen (§ 26 Abs. 2 S. 1 BDSG).[41] Dass in einem Arbeitsverhältnis schon strukturell ein Abhängigkeitsverhältnis besteht, schließt die Freiwilligkeit nicht per se aus.[42] Wenn jedoch die Vereinbarung als Bedingung für den Abschluss des Arbeitsvertrages gestellt wird, ist die Freiwilligkeit zweifelhaft.[43] Freiwilligkeit kann hingegen vorliegen, wenn der

33 Einer über die Grundsätze von Treu und Glauben begründeten Herausgabepflicht steht nicht entgegen, dass möglicherweise strafrechtlich relevante oder kündigungsbegründende Umstände offenbart würden. Der *nemo-tenetur*-Grundsatz betrifft in erster Linie die Situation staatlicher Auskunftsverlangen und findet im Verhältnis zwischen Arbeitgeber und Arbeitnehmer grundsätzlich keine unmittelbare Anwendung, vgl. *Spehl/Momsen/Grützner* CCZ 2014, 170 (171); *Lützeler/Müller-Sartori* CCZ 2011, 19 (20). Dies dürfte auf die Situation der Herausgabe möglicherweise belastender Geräte zu übertragen sein.

34 Nach Beendigung des Arbeitsverhältnisses besteht – unabhängig von der Situation interner Investigationen – gem. § 667 BGB ein Anspruch des Arbeitgebers, dienstliche Kontakte oder sonstige in Erfüllung der beruflichen Tätigkeit erlangte Daten an den Arbeitgeber herauszugeben.

35 *Koch* ITRB 2012, 35; vgl. *Göpfert/Wilke* NZA 2012, 765 (769); Forgó/Helfrich/Schneider/*Helfrich*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 46.

36 Es bestehen auch keine weiteren gesetzlichen Herausgabeansprüche; insbesondere ist § 127 StPO nicht einschlägig, vgl. Thüsing/Wurth/*Forst*, Social Media im Betrieb, 2015, Kap. II, Rn. 124. Auch die Möglichkeit zur Selbsthilfe (§ 229 BGB) besteht nicht, da in der Regel kein Fluchtverdacht bestehen dürfte und obrigkeitliche Hilfe rechtzeitig zu erlangen wäre.

37 *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, S. 140.

38 *Kort* RdA 2018, 24 (26).

39 *Klösel/Mahnhold* NZA 2017, 1428 ff.

40 Für einen Überblick über den Streitstand zur alten Rechtslage vgl. zB *Wybitul/Böhm* BB 2015, 2101.

41 *Ströbel/Böhm/Breunig/Wybitul* CCZ 2018, 14 (15 f.).

42 *Düwell/Brink* NZA 2017, 1081 (1084 f.).

43 Kühling/Buchner/*Maschmann*, DS-GVO BDSG, 2. Aufl. 2018, § 26 BDSG Rn. 62 f.

Arbeitnehmer die Wahl zwischen BYOD-Geräten und Geräten des Arbeitsgebers hat.[44] Gerade bei internen Ermittlungen kann eine Freiwilligkeit bisweilen zweifelhaft sein. Während für den Arbeitgeber die schnelle und vollständige Aufklärung des Sachverhaltes das primäre Ziel ist, so dürfte es für den betroffenen Arbeitnehmer im Vordergrund stehen, seine personenbezogen Daten zu schützen.

Wenngleich nach dem neuem Datenschutzrecht eine Einwilligung des Arbeitnehmers eine mögliche Rechtsgrundlage für die Datensichtung ist, gehen mit ihr erhebliche rechtliche Unsicherheiten einher.[45] Es sollte zusätzlich sichergestellt werden, dass die beabsichtigte Verarbeitung in Form des Auslesens und Sichtens bereits nach den gesetzlichen Rechtsgrundlagen der § 26 Abs. 1 S. 1 oder S. 2 BDSG zulässig ist.

b) Datenverarbeitung zur Aufdeckung von Straftaten und sonstigen Pflichtverletzungen, § 26 Abs. 1 BDSG

Eine im Kontext interner Ermittlungen im besonderen Maße relevante Datenverarbeitung zum Zwecke der Aufdeckung von Straftaten darf nur erfolgen, wenn dokumentierte tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat (§ 26 Abs. 1 S. 2 BDSG). Dazu muss zumindest ein durch konkrete Tatsachen belegter einfacher Anfangsverdacht (§ 152 StPO) gegen den betroffenen Arbeitnehmer vorliegen.[46]

Handelt es sich nicht um den Verdacht einer Straftat, sondern die Aufklärung einer möglichen (Compliance-) Pflichtverletzung aus dem Arbeitsverhältnis, ist ein Rückgriff auf § 26 Abs. 1 S. 1 BDSG möglich, der eine Datenverarbeitung im Rahmen des Beschäftigungsverhältnisses erlaubt, wenn diese für dessen Durchführung oder Beendigung erforderlich ist.

c) Verhältnismäßigkeit der Datenverarbeitung

Eine Datenverarbeitung muss stets erforderlich und im konkreten Einzelfall verhältnismäßig sein (§ 26 Abs. 1 S. 1, S. 2 BDSG). Daneben gilt der Verhältnismäßigkeitsgrundsatz nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO als allgemeines datenschutzrechtliches Prinzip.[47] Für die Sichtung von BYOD-Geräten gelten hierbei besonders hohe Anforderungen.

Während Erforderlichkeit nur gegeben ist, wenn keine milderen, gleich geeigneten Mittel zur Verfügung stehen, um den vermuteten Verstoß aufzudecken,[48] ist im Rahmen der Verhältnismäßigkeit eine Interessenabwägung vorzunehmen. Dabei sind das allgemeine Persönlichkeitsrecht des Arbeitnehmers in Ausprägung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) und das Interesse des Arbeitgebers an der Datenverarbeitung zur Aufklärung von Gesetzes- oder Compliance-Verstößen in Ausgleich zu bringen. Beide Interessen müssen zur Herstellung praktischer Konkordanz gegeneinander abgewogen werden.[49]

Bei BYOD-Geräten ist die Eingriffsintensität im Fall von internen Ermittlungen besonders hoch. Es handelt sich um ein im Privateigentum des Arbeitnehmers stehendes Gerät. Es ist damit wahrscheinlicher als bei einem geschäftlichen Endgerät, dass sich auf diesem Daten, Bild- und Textdateien befinden, die der Privat- oder sogar der Intimsphäre zuzuordnen sind. Letztere markiert den Kernbereich privater Lebensführung und ist für die Betriebsparteien tabu.[50] An die Verhältnismäßigkeit des Sichtens und Auslesens der Daten sind daher gesteigerte Anforderungen zu stellen. Durch technische Vorkehrungen sollte sichergestellt werden, dass nur solche Daten ausgelesen werden, die potentiell einen Bezug zu dem aufzuklärenden Sachverhalt haben können. Auf das pauschale Auslesen bspw. der Bildergalerie des Geräts ist zu verzichten, wenn nicht besondere Anhaltspunkte hierfür vorliegen. Chatprotokolle sind zwar nicht pauschal der Intimsphäre zuzuordnen und dürfen grundsätzlich beim Auslesen erfasst und gesichtet werden,[51] jedoch kann dies im Einzelfall unverhältnismäßig sein, selbst wenn es sich um Chatprotokolle zwischen Beschäftigten handelt.

Maßgeblichen Einfluss auf die in der Verhältnismäßigkeitsprüfung gebotene Abwägung hat zudem die besondere Interessenlage der Beteiligten einer BYOD-Vereinbarung. So bringt der Arbeitnehmer das in seinem Privateigentum stehende Endgerät in das System des Arbeitgebers ein und öffnet hierdurch einen wesentlichen Teil seiner Privatsphäre. Hierdurch kommt er nicht nur dem Interesse des Arbeitgebers nach, sondern setzt sich, sein Gerät und seine Daten auch in gesteigerter Form der Zugriffsmöglichkeit seines Arbeitgebers aus. Der Arbeitnehmer erscheint daher besonders schutzbedürftig. In BYOD-Konstellationen dürfte daher ein strengerer Verhältnismäßigkeitsmaßstab gelten als bei der Nutzung von Endgeräten des Arbeitgebers.

2. Rechtliche Risiken bei unzulässiger Datenverarbeitung

Sollte der Arbeitgeber ohne oder außerhalb der Grenzen einer Ermächtigungsgrundlage Daten des Arbeitnehmers verarbeiten, verletzt er möglicherweise seine Fürsorgepflicht aus dem Arbeitsvertrag und kann sich unter Umständen schadensersatzpflichtig machen (§§ 611 Abs. 1, 280 Abs. 1, Abs. 2, 241 Abs. 2 BGB).[52] Daneben bestehen die erheblichen Bußgeldrisiken der DSGVO, die bis zu 20 Mio. EUR oder 4 % des weltweit erzielten Jahresumsatzes ausmachen können (Art. 83 Abs. 5 DSGVO).

Bei einem heimlichen Auslesen der Daten des BYOD-Geräts kommt eine Strafbarkeit nach §§ 202 a, 202 c StGB in Betracht. Die hierfür erforderliche Überwindung besonderer Zugangssicherungen ist jedoch nicht gegeben, wenn der Arbeitgeber mittels Serverkennworts direkten Zugriff auf die dienstlichen Daten der Arbeitnehmer hat.[53]

---

44 Vgl. *Kort* RdA 2018, 24 (30).
45 So auch *Ströbel/Böhm/Breunig/Wybitul* CCZ 2018, 14 (16).
46 *Benkert* NJW-Spezial 2018, 562; Kühling/Buchner/*Maschmann*, DS-GVO BDSG, 2. Aufl. 2018, § 26 BDSG Rn. 58 ff.
47 Nach dem „Grundsatz der Datenminimierung" muss die Verarbeitung darüber hinaus stets dem Zweck angemessen sowie auf das für die Zwecke notwendige Maß beschränkt sein, Art. 5 Abs. 1 lit. c) DSGVO.
48 Hierzu können etwa Interviews mit den betroffenen Mitarbeitern zählen.
49 BT-Drs. 18/11325, S. 97.
50 Kühling/Buchner/*Maschmann*, DS-GVO BDSG, 2. Aufl. 2018, § 26 BDSG Rn. 41 ff.
51 Vgl. LAG Hamm 10.7.2012 – 14 Sa 1711/10 = CCZ 2013, 115.
52 *Badziura*, Private und dienstliche Internetnutzung, 2016, S. 79.
53 In diesem Fall ist § 202 a StGB auch nicht anwendbar, wenn der Beschäftigte ein Passwort verwendet hat, da dieses dann nicht den Zweck verfolgt, den Arbeitgeber am Datenzugriff zu hindern; vgl. Rotsch/*Eisele*, Criminal Compliance, 2015, § 23 Rn. 39.

Eine unbefugte Aufzeichnung und Mitteilung privater Daten durch den Arbeitgeber im Zuge interner Ermittlungen kann ferner eine Verletzung des Post- und Fernmeldegeheimnisses darstellen, § 206 StGB.[54] Voraussetzung ist, dass das Unternehmen als Anbieter von Telekommunikationsdienstleistungen dem Fernmeldegeheimnis nach § 88 TKG unterliegt. Jedenfalls in der Situation des POCE-Modells, in der die SIM-Karte des Endgeräts nicht von dem Arbeitgeber zur Verfügung gestellt, sondern zusammen mit dem BYOD-Gerät durch den Arbeitnehmer eingebracht werden dürfte, scheidet eine Eigenschaft des Arbeitsgebers als Dienstanbieter iSd Art. 88 TKG jedoch regelmäßig aus. Hier erlaubt und ermöglicht dieser nicht die private Nutzung dienstlicher Geräte und SIM-Karten, sondern vielmehr die dienstliche Nutzung der privaten Geräte des Arbeitnehmers.[55]

Neben den strafrechtlichen Risiken läuft der Arbeitgeber bei Verstößen gegen die gesetzlichen Vorschriften Gefahr, die erlangten Informationen vor Gericht nicht verwerten zu können.[56] Bei Verletzungen des Allgemeinen Persönlichkeitsrechts nimmt die Rechtsprechung grundsätzlich ein prozessuales Verwertungsverbot an.[57] Anderes gilt nur, wenn eine Güterabwägung im Einzelfall ergibt, dass das geschützte Beweisführungsinteresse gegenüber dem verletzten Persönlichkeitsrecht Vorrang genießt.[58]

D. Fazit

Der Zugriff auf die Kommunikation von Arbeitnehmern stellt für Unternehmen im Zuge interner Untersuchungen eine wesentliche Erkenntnisquelle zur Aufdeckung von möglichen Compliance-Verstößen dar.

Um rechtmäßig auf die Daten eines BYOD-Geräts zugreifen zu können, sollten Unternehmen zunächst eine technische Trennung zwischen dienstlichen und privaten Daten der Arbeitnehmer anstreben. Ferner bedarf es in der Regel eines Anspruchs auf Herausgabe des Geräts, der möglichst explizit für die Fälle interner Ermittlungen vereinbart werden sollte. Schließlich sind für eine zulässige Sichtung der Daten die datenschutzrechtlichen Grenzen zu beachten.

Insgesamt zeigt sich, dass die Besonderheiten von BYOD und die rechtlichen Beziehungen des Arbeitnehmers zu seinem BYOD-Gerät zu gesteigerten technischen und rechtlichen Herausforderungen führen – sowohl was die Zugriffsmöglichkeiten auf das Gerät als auch die datenschutzrechtlichen Zulässigkeit der Sichtung und Verarbeitung von Daten betrifft.

Auch die Anforderungen der DSGVO können die Durchführung interner Ermittlungen im Kontext von BYOD erschweren. Zumal bei unrechtmäßigen Datenzugriffen des Arbeitgebers nicht nur empfindliche Bußgelder und Schadensersatzforderungen, sondern auch Strafbarkeitsrisiken und prozessuale Beweisverwertungsverbote im Hinblick auf die erlangten Daten drohen.

Es ist damit zu rechnen, dass die Verbreitung von BYOD-Geräten in Unternehmen in Zukunft weiter zunehmen und sich die Fragen einer zulässigen Datenauswertung bei internen Ermittlungen vermehrt stellen werden. Angesichts der aufgezeigten tatsächlichen und rechtlichen Herausforderungen und Risiken sollten Unternehmen entsprechende Vereinbarungen im eigenen Interesse stets im Vorfeld rechtlich absichern. Hierbei sollte neben der Gewährleistung einer effektiven Aufklärung von Compliance-Verstößen auch sichergestellt werden, dass die Rechte der Arbeitnehmer im Falle interner Ermittlungen gewahrt bleiben.

KONTAKT:

Dr. Stefan Bartz
Latham & Watkins LLP
Warburgstraße 50
20354 Hamburg
Tel.: 040/414030
stefan.bartz@lw.com

Dr. Marco Grotenrath
Latham & Watkins LLP
Warburgstraße 50
20354 Hamburg
Tel.: 040/41403161
marco.grotenrath@lw.com

54 Vgl. *Schuster* CR 2014, 21 mit einer umfassenden Übersicht zum Schrifttum (Fn. 10 f.); *Fülbier/Splittgerber* NJW 2012, 1995.
55 *Kort* RdA 2018, 24 (30); vgl. auch Kramer/*Hoppe* IT-Arbeitsrecht, 2017, Kap. B, Rn. 634.
56 Hierzu ausführl. jurisPK-Internetrecht/*Braun*, 4. Aufl. 2014, Kap. VII Rn. 135 ff.
57 BAG 29.10.1997 – 5 AZR 508/96 = AP BGB § 611 Persönlichkeitsrecht Nr. 27; OLG Karlsruhe 25.2.2000 – 10 U 221/99 = NJW 2000, 1577 f.
58 Vgl. dazu *Grobys* NJW-Spezial 2005, 273 (274 mwN).

RECHTSANWÄLTE PROF. DR. THOMAS GRÜTZNER UND TARIK GÜNGÖR*

Aktuelle Entwicklungen in den USA

Die USA gelten als das Land der unbegrenzten Möglichkeiten. Von den USA gehen jedoch auch die größten Sanktions-Risiken für international tätige Unternehmen aus. Dieser Beitrag knüpft an die Beiträge aus den letzten CCZ Ausgaben an (CCZ 2019, 45 ff.; 59 ff.; 139 ff.). In dieser Ausgabe stehen vor allem die neuen Anforderungen an Compliance-Programme im Mittelpunkt.

A. Einleitung

Am 30.4.2019 hat das Department of Justice („DOJ") seine neue Richtlinie für Compliance-Programme veröffent-

* *Thomas Grützner* ist Partner und *Tarik Güngör* ist Associate in der White Collar-Praxis der internationalen Rechtsanwaltssozietät Latham & Watkins LLP.