von **Dr. Sebastian Kraska**

Bring-Your-Own-Device: Datenschutz-Empfehlungen und technische Umsetzungsmöglichkeiten

Smartphone und Tablet sind für viele Nutzer kaum noch aus dem Alltag wegzudenken und bewähren sich als ständige Begleiter für Freizeit und Beruf. Damit neigen sich auch die Zeiten ihrem Ende, in denen nur privilegierte Mitarbeiter Zugriff auf das geschäftliche Kommunikationsgeschehen und Unternehmensdaten von unterwegs erhielten. Der folgende Beitrag erläutert welche datenschutzrechtlichen und technischen Rahmenbedingungen Unternehmen beachten sollten, wenn der Einsatz privater Smartphones im Unternehmen beabsichtigt wird (abgekürzt "Bring-Your-Own-Device" oder "BYOD").

Ein Beitrag von **Peter Meuser (unabhängiger IT-Berater)** und Dr. Sebastian Kraska (Rechtsanwalt und externer Datenschutzbeauftragter).

Warum ist das Datenschutzrecht überhaupt relevant?

Ein Unternehmen bleibt (als so genannte "verantwortliche Stelle" nach § 3 Abs. 7 BDSG) auch dann für die ordnungsgemäße Verarbeitung von personenbezogenen Daten haftungsrechtlich verantwortlich, wenn diese Verarbeitung auf privaten Smartphones der Beschäftigten stattfindet. Aber anders als bei Smartphones, die Eigentum des Unternehmens sind, hat das Unternehmen ohne vorhergehende Vereinbarungen dabei nur eingeschränkte Möglichkeiten, technische und organisatorische Vorgaben hinsichtlich der sicheren Datenverarbeitung auf Privatgeräten zu treffen und diese auch durchzusetzen.

Empfehlung: Vorab Regelung mit Beschäftigten treffen

An sich lautet die Empfehlung daher, im Unternehmen grundsätzlich nur unternehmenseigene Hardware einzusetzen. Sollen in einem Unternehmen dennoch auch private Smartphones Einsatz finden ist es rechtlich unerlässlich, insbesondere zur Vermeidung von Haftungsproblemen, zur Entschärfung möglicher Konflikte bspw. mit dem Fernmeldegeheimnis und zur Sicherstellung einer ordnungsgemäßen Verarbeitung von Geschäftsdaten auf Privatgeräten zu Beginn eine schriftliche Regelung mit den Beschäftigten zu treffen. Der folgende Katalog enthält die zentralen Themen, welche in einer solchen Regelung beinhaltet sein sollten:

Vorgabe zur Trennung privater und geschäftlicher Daten

Zur Meidung von Zugriffsrestriktionen (**insb. durch das Fernmeldegeheimnis in Bezug auf private E-Mails**) sollten private und geschäftliche Daten möglichst klar voneinander getrennt werden.

Diese Trennung stellt die zentrale Anforderung, die es innerhalb einer BYOD-Strategie zu lösen gilt. Alle heute verbreiteten und aktiv fortentwickelten Smartphone-Plattformen wie Apple iPhone (iOS), Google Android, RIM BlackBerry und Microsoft Windows Phone bieten grundsätzlich die Möglichkeit, mehrere Mail-Konten "getrennt" voneinander auf einem Gerät zu verwalten. Unternehmen nutzen als "Messaging System", das auch geschäftliche Kalender- und Kontaktdaten zur Synchronisation auf dem Smartphone bereitstellt, meist Microsoft Exchange ("Outlook") oder Lotus Domino ("Lotus Notes").

Ohne weitere Maßnahmen kann allerdings kaum von einer "sauberen" Trennung privater und geschäftlicher Daten die Rede sein. Beide Bereiche werden zunächst gleichberechtigt auf den Geräten behandelt. Kommt ein ungeschütztes Privatgerät mit geschäftlichen Daten in fremde Hände, liegen daher beide Bereiche gleichermaßen offen. Werden private Mails über das Firmen-Mail-Konto weitergeleitet, geraten sie in das Kontrollsystem des Messaging Systems im Unternehmen (z.B. gesetzliche Mail-Archivierung). Umgekehrt besteht ebenso das Risiko Firmendaten unkontrolliert über das Privatkonto weiterzuleiten. Privat installierte Apps auf den Smartphones können (je nach Mobilplattform) vom Anwender unbemerkt Zugriff auf Mail-Konten erhalten und leiten vertrauliche Information selbsttätig nach außen.

Sobald ein Privatgerät mit der Unternehmens-IT verbunden wird, gilt es diese Risiken zu kontrollieren, minimieren und möglichst zu unterbinden. iPhones, BlackBerries, wie auch Geräte unter Android und Windows Phone bringen dazu von Haus aus bereits unterschiedliche Voraussetzungen mit, auf die verschiedene Ansätze zum "Mobile Device Management" (MDM) aufsetzen (siehe vertiefend["](http://www.itlab.de/s/mdmov) **Überblick: Kontrollmöglichkeiten der aktuellen Mobilplattformen im Unternehmenseinsatz"**).

Regelung zum Zugriff auf Daten

Es sollte mit dem Beschäftigten vorab vereinbart werden, wer wie wann und in welcher Form seitens des Unternehmens (Fern-)Zugriff auf die Daten des Smartphones nehmen kann. Rechtlicher Hintergrund: Jede verdeckte Datenverarbeitungsmaßnahme wiegt rechtlich schwerer als eine offene/transparente Datenverarbeitungsmaßnahme und ist daher datenschutzrechtlich schwerer zu rechtfertigen.

Denkt man bei der technischen Implementierung dabei zunächst an Daten, die unmittelbar auch das Persönlichkeitsrecht betreffen wie die Fernerhebung von Gesprächs- und Ortungsdaten, so lassen sich bei modernen Smartphones eine Fülle weiterer privater Daten auslesen, die im Kontext von IT-Richtlinien relevant sind. Dazu gehört die zentrale Inventarisierung privat installierter Apps, wie auch Informationen über private Mail-, WiFi- und VPN-Konfigurationen, sowie der Roaming-Status zur Erkennung von Auslandsaufenthalten. Selbst die Version des eingesetzten Smartphone-Betriebssystems kann aufgrund von spezifischer Sicherheitsrisiken zum Ausschluss von der Unternehmensanbindung herangezogen werden und sollte in der Vereinbarung über erhobene Daten nicht fehlen.

Neben dem passiven Auslesen von Gerätedaten ermöglichen Systeme wie die BlackBerry Enterprise Solution auch die aktive Installation von Apps und damit einen beeinflussenden Fernzugriff. iPhone und Android-basierte Geräte erlauben dies grundsätzlich nur durch Aufforderung des Nutzers. Eine vollständige Fernsteuerung der beiden Mobilplattformen zu Support-Zwecken wird von MDM-Lösungen derzeit nicht unterstützt und wäre auch nur durch explizite Bewilligung des Nutzers im Einzelfall zulässig.

Regelung zur Frage "Wann darf das Unternehmen Daten löschen?"

Insbesondere im Verlustfall des Smartphones (u.U. auch bei streitigem Ausscheiden des Beschäftigten) kann es wünschenswert sein, die auf dem Smartphone gespeicherten Daten per Fernbefehl löschen zu lassen. Von diesem Löschbefehl wären dann - je nach Betriebssystem und eingesetzter MDM-Lösung - auch private Daten des Beschäftigten betroffen. Hier empfiehlt sich daher eine Regelung im Vorfeld.

Bereits die Standardmöglichkeiten der gängigsten Messaging-Plattformen erlauben prinzipiell auch ohen zusätzliche MDM-Mechanismen eine vollständige Gerätelöschung, solange noch eine Verbindung zum Gerät zwecks Datensynchronisation aufgebaut wird. Der Trend geht aber eindeutig dahin, nicht nur technisch für eine saubere Trennung zwischen privaten und geschäftlichen Daten auf den Geräten zu sorgen, sondern die Unternehmensdaten selektiv löschen zu können. Konsequent umsetzen kann dies heute z.B. das Unternehmen RIM mit "BlackBerry Balance" (nur BlackBerry-Geräte) und das Unternehmen Good Technology für iOS (iPhone/iPad), Android und (eingeschränkt) Windows Phone. Auch Apple gibt

seiner profilbasierten MDM-Spezifikation Möglichkeiten mit auf den Weg, um Unternehmens-Mail-Konten zusammen mit anderen zentral verteilten Konfigurationseinstellungen gezielt von Geräten entfernen zu können. Dies wird von MDM-Lösungen der Anbieter AirWatch und MobileIron aufgegriffen und umgesetzt. Integrierte "Self-Service-Portale" erlauben dem Nutzer Maßnahmen dieser Art - z.B. im Verlustfall - auch selbsttätig anzustoßen. Bereits bei der Aktivierung der MDM-basierten Administrationseinbindung bestätigt der Nutzer im Bildschirmdialog explizit, in welchem Umfang Daten auf seinem Gerät durch die IT gelöscht werden können.

Recht des Arbeitgebers, mit Privatgerät in gleicher Weise wie mit Unternehmensgerät zu verfahren

Anschließend an den Punkt "Wann darf das Unternehmen Daten löschen?" empfiehlt sich aus Sicht der Arbeitgeber eine klarstellende Regelung, dass der Arbeitgeber mit dem privaten Smartphone des Beschäftigten grundsätzlich in gleicher Weise verfahren darf wie mit betrieblicher Hardware.

Dies betrifft bei der Umsetzung insbesondere auch die Reglementierung bzw. Deaktivierung spezifischer Gerätefunktionen. Das mögliche Spektrum reicht dabei von Deaktivierung von Internet-basierter Spracherkennung über Apples "Siri" (wird so von IBM intern praktiziert), dem Unterdrücken der automatischen Datensicherung über Cloud-Dienste bis hin eine App-Installation nur aus einem unternehmensinternen Katalog und nicht den öffentlichen App Stores von Apple und Google zuzulassen. Wie wirksam solche Regelungen auch technisch umgesetzt werden können, hängen von Smartphone-Betriebssystem und darauf aufsetzender MDM-Lösung ab.

Regelung zum Einsatz von Monitoringtools

Beim Einsatz (technisch empfehlenswerter) Monitoringtools zur Überwachung des korrekten Systemzustandes und der zulässigen Systemverwendung sind datenschutzrechtlich insbesondere zwei Punkte zu beachten: a) die Art und Weise der Datenverarbeitung und der damit verbundene Zweck muss zu Beginn transparent beschrieben werden. b) Beim Einsatz von Software bei (vor allem außer-europäischen) Drittdienstleistern müssen die insoweit geltenden Datenschutzvorgaben beachtet werden (vgl. vertiefend unter **http://www.iitr.de/so-funktioniert-internationaler-datenschutz.html**).

Die kontinuierliche Aufzeichnung von Überwachungsdaten zu Endgeräten stellt von je her insbesondere bei Produkten amerikanischer Herkunft einen Bereich dar, den es besondere Aufmerksamkeit zu schenken gilt. So werden beispielsweise Gesprächsdaten und aufgerufene Internet-Seiten standardmäßig von der BlackBerry-Unternehmenslösung aufgezeichnet, wenn diese nicht ausdrücklich durch den Administrator ausgeschaltet werden. Im Kontext von Privatgeräten gibt es für das Sammeln dieser Daten kaum ein

begründbares Erfordernis. Selbst die durchaus nützliche Möglichkeit zur Geräteortung bei Verlust, wie sie AirWatch und MobileIron für iPhones und Androids anbieten, sollte vor Aktivierung mit den Geräteinhabern definitiv vereinbart werden. Letztlich bestimmen Regelungen zur Kostenübernahme, ob die Aufzeichnung des Roaming-Status von Privatgeräten überhaupt notwendig ist. Zu beachten ist, dass die Aufzeichnung auch unverfänglich wirkender und für den Support-Fall nützlicher Informationen (z.B. die Erhebung der letzten Verbindung zwischen Endgerät und Unternehmens-IT) nicht grundsätzlich auch im Interesse des Gerätebesitzers liegen muss. Dieser sieht sich allzu leicht in der Erklärungssituation, warum geschäftliche E-Mails unbeachtet blieben, obwohl diese ganz offensichtlich technisch seinen digitalen Begleiter erreicht haben.

Sobald die Firmenanbindung eines Privatgeräts an durch den Nutzer veränderbaren Sicherheitseinstellungen wie Aktivierung eine Gerätekennworts vordefinierter Güte, Aktivierung der Geräteverschlüsselung und Nicht-Vorhandensein von Apps einer unternehmensgeführten "schwarzen" Liste gebunden wird, ist deren regelmäßige Erfassung und Abgleichung mit sich durchaus verändernden zentralen Regelwerken unumgänglich. Ein besonderer Augenmerk liegt dabei auf der Erkennung eines Jailbreak (iPhone) bzw. Rooting (Android). Smartphones in diesem Zustand können jenseits der von den Herstellern vorgesehen Möglichkeiten eingesetzt werden, um z.B. unautorisierte Software zu betreiben. Dieser bei Privatanwendern beliebte Weg zur Funktionserweiterung kann im Unternehmenskontext aus Sicherheitsgründen aber nicht geduldet werden. Ohne Bereitschaft des Nutzers zur Überwachung seines Privatgeräts im vereinbarten Rahmen, sind die meisten MDM-Lösungen nicht einsatzfähig. Im BYOD-Einsatzszenario reagieren die meisten MDM-Lösungen bei erkannter Verletzung der Sicherheitsrichtlinien mit automatischen Maßnahmen. Diese reichen im einfachsten Fall von einer rein passiven Benachrichtigung des Nutzers und zuständiger IT-Stellen, über die aktive Unterbrechung der Mail-Synchronisation bis der Nutzer selbstständig die Regelkonformität wieder hergestellt hat, bis hin zur Löschung aller Unternehmensdaten. Da die IT-Sicherheitsrichtlinien durchaus dynamischer Natur sind, muss die Überschreitung von zeitlichen Grenzwerten bei der regelmäßigen Kontaktaufnahme zwischen Smartphone und MDM-Lösung vom System überwacht werden.

Auch hier tritt der Ansatz des Unternehmens Good Technology hervor, indem optional auf eine "klassische" Geräteverwaltung und somit -überwachung unter iOS und Android - obwohl vorhanden - verzichtet werden kann. Unternehmensdaten verbleiben in sich geschlossenen (und verschlüsselten) App-Containern, die bei diesem Ansatz keinerlei direkten Austausch mit anderen Apps auf dem Gerät zulassen. Der App-Container tauscht sich mit der Unternehmens-IT über einen dedizierten, verschlüsselten Kanal aus. Auf diese Weise sind dann auch vom Nutzer kontrollierte Einstellungen für die Gewährleistung eines sicheren Betriebs nicht mehr im gleichen Masse ausschlaggebend und können wesentlich großzügiger gehandhabt werden.

Vorgaben zur festen Einstellung von Systemparametern

Es empfehlen sich schriftlich festgehaltene Vorgaben, dass der Beschäftigte bei seinem Smartphone bestimmte Sicherheitseinstellungen vorzunehmen hat bzw. diese (einmal eingestellt) nicht mehr verändern darf (wie z.B. Regelungen zur Passwortvergabe, automatisches Ausschalten des Smartphones, Zulässigkeit der Ortung im Verlustfall etc.).

Wie bereits beschrieben, stellt die technische Definition von Richtlinien zum sicheren Betrieb sowie die Überwachung deren Einhaltung zwar das Grundgerüst von MDM-Lösungen dar, doch fällt die Information der Nutzer durch die heutigen Systeme über vorzunehmende Einstellungen oder Verstöße gegen Vorgaben meist zu kryptisch und unverständlich aus. In der Praxis sollte eine individuell auf die Firmensituation abgestimmte Dokumentation, einführendes Training der Beschäftigten an ihren privaten Geräten und geschultes Support-Personal eingeplant werden. Da sich die Gewährleistung von Datenschutz und -sicherheit in einem dynamischen Kontext bewegt, gilt es nicht nur eine statische Startsituation zu schaffen, sondern vielmehr einen Prozess zu etablieren, der die jeweils aktuelle Situation effizient zu dokumentieren hilft und diese Informationen auch leicht konsumierbar den Beschäftigten bereitstellt.

Regelung zur Haftungsverteilung

Zur Meidung späterer Rechtsstreitigkeiten ist grundsätzlich zu empfehlen, bereits zu Beginn eine Regelung zur Haftungsverteilung zwischen Arbeitnehmer und Arbeitgeber zu treffen.

Mitteilungspflicht bei Verlust

Von besonderer Wichtigkeit (insb. im Hinblick auf Informationspflichten des Unternehmens im Datenverlustfall nach § 42a BDSG) ist die Pflicht des Arbeitnehmers, im Verlustfall des Smartphones unverzüglich den Arbeitgeber zu informieren.

Diese organisatorische Maßnahme unterstützen MDM-Lösungen auch mit den bereits erwähnten "Self-Service-Portalen". Hierüber kann der Beschäftigte von einem beliebigen PC mit Internet-Anschluss sowohl Kontakt mit dem Helpdesk aufnehmen, um auf formalisierten Weg seine Meldung abzusetzen, als auch gleich selbst zur Tat schreiten, indem er versucht sein Gerät zu orten oder fernzulöschen.

Nutzung des privaten Smartphones durch Dritte

Für den Arbeitgeber empfehlenswert wäre zudem eine Regelung, die Nutzung des privaten Smartphones durch sonstige Dritte (Freunde, Familie des Beschäftigten) zu untersagen um sicherzustellen, dass wirklich nur der Berechtigte selbst Zugriff auf Unternehmensdaten nehmen kann.

Der Schutz von Unternehmensdaten bei der bewussten Weitergabe des Privatgeräts an Dritte kann technisch nur unterstützt werden, indem der Zugriff auf Geschäftsdaten unabhängig vom sonstigen Gerät mit einem eigenen Kennwort geschützt wird. "Good for Enterprise" implementiert dies z.B. für die eigene Mail-App, deren Daten auch unabhängig von einer aktivierten Geräteverschlüsselung eigens verschlüsselt werden (vgl. saubere Trennung von Privat- und Geschäftsdaten).

Durchführung von Reparatur und Wartungsarbeiten

Arbeitgeber und Arbeitnehmer sollten Regelungen hinsichtlich der regelmäßigen Durchführung von Reparatur und Wartungsarbeiten (Einspielen von Updates durch die IT-Abteilung, keine Weitergabe des Smartphones an Reparaturwerkstätten etc.) treffen.

Muss ein Gerät z.B. im Reparaturfall für längere Zeit an Dritte übergeben werden, empfiehlt sich grundsätzlich die Daten darauf zu sichern und sensible Daten zu löschen. Erlaubt die im Einsatz befindliche MDM-Lösung die Firmenkonfiguration auf Knopfdruck gezielt zu löschen (Standardmöglichkeit bei Apple-MDM) und das Gerät auch ohne Helpdesk-Unterstützung prinzipiell wieder in die Unternehmens-IT einzubinden, lässt sich diese Vorgehensweise auch in der Mitarbeitervereinbarung festhalten. Die meisten MDM-Lösungen erfordern Smartphone-seitig nur die Angabe von drei Angaben in der MDM-App, um das Privatgerät im Unternehmen zu registrieren: Name des MDM-Servers, Benutzerkennung (entspricht meist Windows-Kennung im Unternehmen) und (Windows-)Passwort. Auf diesem Hintergrund reicht es meist bereits, lediglich die Weitergabe des Smartphone mit Unternehmensdaten an Dritte zu untersagen.

Fazit

Gestatten Unternehmen die Nutzung privater Smartphones für das Unternehmen, bleiben sie haftungsrechtlich für die Datenverarbeitung auf diesen Geräten verantwortlich, haben aber im Zweifel keine Möglichkeit, auf das Gerät zuzugreifen. Sollen in einem Unternehmen dennoch auch private Smartphones eingesetzt werden, ist aus rechtlicher Sicht eine vorherige Regelung mit den Beschäftigten zu treffen, um eine noch vertretbare Balance zwischen Haftungsrisiken einerseits und Vorteilen aus der Verwendung privater Smartphones andererseits zu finden.

Wie sich die Vereinbarungen zum geschäftlichen Einsatz privater Geräte auch mit technischen Maßnahmen unterstützen lassen, hängt einerseits von den Smartphone-Modellen ab, die im IT-Kontext akzeptiert werden und andererseits von der ausgewählten Lösung zum Mobile Device Management. BYOD lässt sich heute nicht generell und mit beliebigen Geräten ohne Sicherheitsrisiko für das Unternehmen oder Datenschutzbedenken gegenüber dem Beschäftigten umsetzen. Die meisten Möglichkeiten bieten heute noch die Verwaltungsfunktionen von iPhone und iPad, die Apple seinen Geräten seit iOS 5 von Haus aus mit auf den Weg gibt. Den konsequentesten Ansatz zum Trennen privater und geschäftlicher Daten auch für Android und Windows Phone findet sich heute bei den Produkten des Unternehmens Good Technology. Aber auch diese Lösung passt nicht auf jede Unternehmenssituation und sollte daher vor einem Einsatz genau geprüft werden.

Unabhängig von der letztlich eingesetzten technischen Lösung sollten zusammen mit den Datenschutzvereinbarungen alle IT-Aktivitäten auf Privatgeräten genau und für den Mitarbeiter transparent dokumentiert werden. Durch die Dynamik dieser Aufgabe empfiehlt es sich einen effektiven und pflegeleichten Dokumentationsprozess zu etablieren. Dieser kann z.B. auch Teil eines "mobilen" Intranets des Unternehmens sein.

Über die Autoren

Herr Peter Meuser hat sich als unabhängiger IT-Berater auf mobile Lösungen für den Unternehmenseinsatz spezialisiert und unterstützt Firmen bei der Strategieentwicklung, herstellerneutralen Produktauswahl und Lösungsimplementierung. Weitergehende Infos zum Thema und den direkten Kontakt finden Sie unter http://www.itlab.de.

Herr Rechtsanwalt Dr. Sebastian Kraska (http://www.iitr.de) ist auf den Bereich des betrieblichen Datenschutzrechts spezialisiert und betreut gemeinsam mit einem Team von Regionalpartnern Unternehmen im gesamten Bundesgebiet als externer Datenschutzbeauftragter.

Autor:
Dr. Sebastian Kraska
Rechtsanwalt