SIMPLY SECURE

Mobile Device Management

Umgang mit personenbezogenen Daten in Deutschland – heute und morgen

G DATA Software AG | Januar 2016

1. Grundsätzliches

Ein nicht nur im Mittelstand relativ wenig bekannter Umstand ist, dass nach zwingendem deutschem und europäischem Recht der Umgang mit personenbezogenen Daten grundsätzlich verboten ist. Es gilt hier ein „Verbot mit Erlaubnisvorbehalt“. Ins Normaldeutsche übersetzt heißt das: Persönliche Daten einer natürlichen Person dürfen nur verarbeitet werden, wenn eine Erlaubnis dafür vorliegt. „Juristische Personen“ wie etwa eine GmbH sind hier ausdrücklich nicht eingeschlossen. Personenbezogene Daten können neben Namen und Adressen auch „sensible“ Daten enthalten, die etwa Informationen über eine Gewerkschaftszugehörigkeit oder religiöse Überzeugungen, die Ethnie, die Gesundheit sowie sexuelle oder politische Präferenzen umfassen. Ein verbreiteter Irrglaube besteht darin, dass es auf die Schutzwürdigkeit, bzw. die Sensibilität der Daten ankäme. Die Verarbeitung sämtlicher personenbezogener Daten ist jedoch generell strikt verboten, sofern keine konkrete Erlaubnis vorliegt. Zuwiderhandlungen werden bereits jetzt als Ordnungswidrigkeit und ggf. als Straftat verfolgt.

2. Rechtslage

Eine Erlaubnis zur Verarbeitung personenbezogener Daten kann entweder in Form einer Einwilligung des „Betroffenen“ (also demjenigen, dessen Daten verarbeitet werden sollen) oder als gesetzliche „Erlaubnisnorm“ vorliegen. Bei der Einwilligung ist zu beachten, dass das Bundesdatenschutzgesetz (BDSG) bestimmte Anforderungen an die Form und den Inhalt der Einwilligung für ihre Wirksamkeit stellt. Diese Anforderungen muss derjenige, der diese Daten erhebt, (im Juristendeutsch „verantwortliche Stelle“ genannt) erfüllen. In Form von gesetzlichen Erlaubnissen gibt es Vorschriften, auf deren Grundlage in einer ganzen Reihe von bestimmten Konstellationen Daten verarbeitet werden dürfen, ohne oder auch gegen den Willen des Betroffenen.

Wichtig ist, dass man vorher prüft, ob man für eine bestimmte Datenverarbeitung eine Einwilligung benötigt oder ob es eine gesetzliche Erlaubnis gibt. So dürfen Händler beispielsweise kraft Gesetzes Namen und Adressen ihrer Kunden verarbeiten – ansonsten könnten sie keine Bestellungen annehmen, keine Waren ausliefern und auch keine Rechnungen erstellen. Es gibt hingegen für einen Händler meistens keinen Grund, Daten über die politische Ausrichtung oder die ethnische Herkunft eines Kunden zu erheben, da diese Daten für die Erfüllung eines geschäftlichen Verhältnisses in der Regel nicht benötigt werden. Sollen allerdings die erhobenen Daten zusätzlich für werbliche Zwecke genutzt werden, benötigen Händler hingegen eine wirksame Einwilligung, denn die Verarbeitung von Daten ist grundsätzlich nur für den Zweck erlaubt, zu dem sie erstmals beschafft wurden. Im Hinterkopf zu behalten ist zudem, dass große Teile der gesetzlichen Grundlagen nicht an aktuelle technische Gegebenheiten angepasst sind. Das aktuelle BDSG stammt überwiegend aus dem Jahre 2001.

In Teilen sind die zugrundeliegenden Regelungen mehr als 25 Jahre alt und stammen damit – zumindest nach Maßstäben der IT-Branche – in mehrfacher Hinsicht aus dem letzten Jahrtausend.

Teilweise wird hier die EU-Datenschutzgrundverordnung (DS-GVO) Abhilfe schaffen. Diese findet nach ihrem Inkrafttreten in allen EU-Mitgliedsstaaten unmittelbare Anwendung, ohne dass die jeweiligen Gesetzgeber noch einmal tätig werden müssten. Bis zum 25. Mai 2018, dem Tag des Inkrafttretens der DS-GVO, haben Unternehmen Zeit, sich auf die neuen Maßstäbe dieser Verordnung auszurichten. Es besteht in vielen Unternehmen dringender Handlungsbedarf, um sich an die künftige Rechtslage anzupassen. Unternehmen, die sich nicht auf die neue Rechtslage einstellen und diesen Stichtag verstreichen lassen, riskieren empfindliche Strafen. Die neue Rechtslage wartet in diesem Zusammenhang mit drastisch verschärften Sanktionen auf.

3. MDM im Kontext der deutschen Rechtsprechung

Mobile Device Management (MDM) gehört mittlerweile zum betrieblichen Alltag in vielen Unternehmen. EDV-Abteilungen benutzen Lösungen, um sowohl unternehmenseigene Geräte zu verwalten als auch Privatgeräte der Mitarbeiter, falls diese zur geschäftlichen Nutzung freigegeben sind („BYOD“). Derartige Lösungen haben oft weitreichende Möglichkeiten zur Kontrolle, die technisch auch durchaus sinnvoll sind und Gewinn bringend eingesetzt werden können. Es gibt jedoch einige juristische Feinheiten, die an dieser Stelle zu beachten sind. Kann eine MDM-Lösung beispielsweise die GPS-Koordinaten eines Gerätes erfassen, so ist beim Nutzen dieser Funktion Vorsicht geboten. Mit einer solchen Funktion können etwa gestohlene oder verlorene Geräte geortet und dem Benutzer wieder zugeführt werden, was eindeutig erstrebenswert ist - allerdings ist hier auch Missbrauch nicht nur denkbar, sondern naheliegend. Dabei ist häufig nicht jede Verwendung, die rechtlich als Missbrauch gewertet wird, auch auf den ersten Blick als solche erkennbar.

4. Grundsatzentscheidungen

Will man sich und seine MDM-Strategie juristisch absichern, müssen durch die Geschäftsleitung zunächst einige Grundsatzentscheidungen getroffen werden. Hierzu gehört auch die Entscheidung, ob die Nutzung von Privatgeräten für geschäftliche Zwecke bzw. die Nutzung unternehmenseigener Geräte für private Zwecke erlaubt wird (und unter welchen Auflagen) oder nicht. Hierzu sind bereits einige wesentliche Dinge zu beachten, die nicht nur mit juristischen, sondern auch rein praktischen Erwägungen zu tun haben:

1. Unternehmenseigene Geräte

Stellt das Unternehmen einem Mitarbeiter ein Mobilgerät, etwa ein Smartphone, Tablet PC oder Notebook zur Verfügung, so ist zu klären, ob eine Nutzung für private Zwecke zulässig ist oder nicht. Ist ausschließlich die dienstliche Nutzung gestattet (gesetzlicher Regelfall), so

sollte das Unternehmen grundsätzlich zumindest stichprobenartig kontrollieren, ob das Verbot der Nutzung zu privaten Zwecken tatsächlich eingehalten wird. Beim Verstoß können entsprechende Sanktionen ergriffen werden, bis hin zur Abmahnung und Kündigung.

Wichtig ist in diesem Zusammenhang auch die Frage, ob der Arbeitgeber jederzeit auf das Gerät - zum Beispiel per Fernzugriff – Zugriff hat bzw. in zulässiger Weise Zugriff nehmen darf. Als verantwortliche Stelle muss er bestimmte technisch-organisatorische Maßnahmen zur Absicherung des Datenschutzes treffen - u.a. die Zugriffsmöglichkeit auf Daten regeln. Ist die private Nutzung gestattet, darf der Arbeitgeber nicht nach Belieben Zugriff auf das Gerät nehmen, da er potenziell Einsicht in private Daten nehmen würde. Dies ist jedoch ohne wirksame Einwilligung nicht zulässig – auch nicht zu dem Zweck, dass der Arbeitgeber die ihm obliegenden gesetzlichen Pflichten erfüllen möchte.

Scheidet der Mitarbeiter aus dem Betrieb aus, hat dieser das Gerät umgehend herauszugeben. Was aber in Fällen der zugelassenen Privatnutzung zu erfolgen hat, sollte besser vertraglich geregelt sein.

2. Privatgeräte und private Speicherplätze

Die dienstliche Nutzung eines Privatgerätes bringt noch einige weitere besondere Herausforderungen mit sich, abgesehen davon, dass regelmäßig auch private Daten auf dem Gerät gespeichert sind. Beim Stichwort „BYOD“ gilt es, einige wesentliche Hindernisse zu meistern. So ist es für Unternehmen u.a. schwierig bis unmöglich, alle Daten lückenlos nachzuverfolgen. Ein rechtssicheres Lizenzmanagement ist schwierig, die technische Trennung von privaten und geschäftlichen Daten als wirksam auszugestalten bisweilen unmöglich.

Hat ein Mitarbeiter Dokumente in einem privaten Cloudspeicher (zum Beispiel Dropbox) abgelegt, so befinden sich diese Daten außerhalb des Zugriffsbereiches des Unternehmens. Neben dem potenziellen Verlust von Geschäfts- und Betriebsgeheimnissen kann dies auch unter dem Gesichtspunkt des Datenschutzes Schwierigkeiten bedeuten, gerade wenn Kundendaten auf diese Weise behandelt werden. Dies gilt in besonderem und verschärftem Maße für bestimmte, zur Verschwiegenheit verpflichtete Berufsstände, wie zum Beispiel Steuerberater, Ärzte oder auch Anwälte (§ 203 StGB).

Erlangt die zuständige Aufsichtsbehörde (zum Beispiel durch eine anonyme Anzeige) Kenntnis davon, dass personenbezogene Daten aus dem geschäftlichen Umfeld außerhalb des Zugriffsbereiches des Betriebs gespeichert werden, drohen Bußgelder und weitere Sanktionen. Hier kann je nach Einzelfall auch der Betrieb bzw. die für den Datenschutz zuständige Person für Verstöße persönlich in Haftung genommen werden.

Fest steht, dass eine Regelung zum Gebrauch von Mobilgeräten schriftlich fixiert werden sollte, zum Beispiel als Anlage zum Arbeitsvertrag. Wer einen Betriebsrat hat, benötigt in der Regel dessen Zustimmung und eine entsprechende Betriebsvereinbarung, weil es sich vielfach um mitbestimmungspflichtige Maßnahmen handeln kann.

Langjährigen Mitarbeitern mit Altverträgen, bei denen beispielsweise die private Nutzung von Unternehmensgeräten nicht ausdrücklich geregelt und geduldet wurde, etwaige Änderungen schmackhaft zu machen, wird nicht einfach sein. Naturgemäß wird es hier Widerstand geben, wenn der lieb gewonnene *status quo* verändert werden soll. Ausnahmen sollten allerdings nicht gemacht werden. Notfalls kann man mit einem Berater über eine Änderungskündigung sprechen. Eine Übergangslösung zu erwägen, kann manchmal den Zwängen der Situation geschuldet sein. Eine solche ist jedoch soweit es geht zu vermeiden. Jedenfalls darf eine Übergangslösung nicht als „dauerhaftes Provisorium“ betrieben werden und so die eigentliche Regelung aushebeln.

5. Risiken und deren Bewertung

In vielen Unternehmen ist die Nutzung von Mobilgeräten durch die Arbeitnehmer nicht ausdrücklich geregelt. Die Nutzung von Privatgeräten für geschäftliche Zwecke bzw. die Nutzung von Unternehmensgeräten im Privatbereich wird jedoch vielfach geduldet. So hat nach einer Gartner-Studie (Studie Nr. G00262545) jeder zweite Smartphone-Benutzer in irgendeiner Form Firmendaten auf seinem Gerät gespeichert.

Eine Richtlinie für die Nutzung von mobilen Endgeräten sollte jedoch in jedem Falle erstellt und umgesetzt werden. Besteht ein unmittelbares Risiko, dass die Vertraulichkeit oder die Integrität von Daten gefährdet ist, muss diesem Umstand Rechnung getragen werden. Bleibt dies aus, so nimmt ein Arbeitgeber Risiken implizit in Kauf, mit allen nachgelagerten Konsequenzen. Dies erstreckt sich bis hin zu persönlicher Haftung bei Datenverlust oder –missbrauch durch Dritte und personellen Konsequenzen. Hat die Unternehmensleitung es beispielsweise versäumt, bestimmten Risiken durch den Einsatz „geeigneter technischer und organisatorischer Mittel“ Rechnung zu tragen, kann das Unternehmen die zur Leitung gehörenden Personen persönlich in Regress nehmen, insbesondere dann, wenn dem Unternehmen durch die Unterlassung ein wesentlicher finanzieller Schaden entstanden ist. Passiert dies in wirtschaftlich schlechten Zeiten, kommt es ggf. dazu, dass ein Insolvenzverwalter derartige Ansprüche aufspürt und verfolgt, zwecks Mehrung der Masse.

Bei diesem Datenverlust oder –missbrauch muss es sich im Übrigen auch nicht immer um Dokumente im klassischen Sinn handeln: auch Fotos von Fertigungsanlagen oder Aufnahmen von bestimmten Stufen eines Fertigungsprozesses können hierunter fallen. Aus diesem Grund sollte auch erwogen werden, den Zugriff auf die Kamera, die heute in den meisten Smartphones eingebaut ist, für bestimmte Bereiche einzuschränken.

6. Was ist zulässig und was nicht?

Beispiel: Ein Mitarbeiter hat sich krankgemeldet. Der Chef vermutet jedoch, dass der Mitarbeiter in Wirklichkeit „blau macht“ und lieber auf Shoppingtour geht. Hier ist die Versuchung gegeben, das Smartphone einmal zu orten und zu schauen, ob der oder diejenige wirklich zuhause ist, wie er behauptet.

Das Problem hier ist allerdings: hat man ein Gerät geortet, ohne den Betroffenen zu informieren und ohne „Erlaubnis“, macht sich die Unternehmensleitung bzw. der Vorgesetzte sehr wahrscheinlich strafbar. Einem angeblich faulen Mitarbeiter aufgrund der gewonnenen GPS-Daten zu kündigen, dürfte ebenfalls schwierig sein. Die erhobenen Daten werden mit sehr großer Wahrscheinlichkeit vor einem Arbeitsgericht nicht als Beweismittel zugelassen. Mangels Einwilligung kommt nur § 32 BDSG als gesetzliche Erlaubnis in Betracht, der insoweit eindeutig ist: Danach ist die Erhebung personenbezogener Daten (zu denen auch Positionsdaten gehören) unter Anderem nur dann zulässig, wenn:

- Im Zuge des Beschäftigungsverhältnisses eine Straftat begangen wurde, bzw. ein entsprechender Verdacht besteht
- es einen durch zu dokumentierende Tatsachen begründeten Verdacht gibt, der die Verarbeitung der Daten rechtfertigt (die ‚Ahnung‘ des Chefs fällt eindeutig nicht hierunter; es müssen tatsächliche Beweise vorliegen!)
- die Verarbeitung der Daten zur Aufdeckung der Tat erforderlich ist (d.h. es gibt kein milderes, gleich effektives Mittel) und
- Art und Ausmaß der Datenverarbeitung im Hinblick auf den Anlass insgesamt nicht unverhältnismäßig sind.

Das „Aufspüren arbeitsunwilliger Mitarbeiter“ ist hiervon in keinem Fall abgedeckt. Das Vorhandensein einer Betriebsvereinbarung kann die Erhebung von Daten über die Beschränkungen des § 32 BDSG hinaus legitimieren, sollte sich zuvor ein Betriebsrat gefunden haben, der einer solchen Vereinbarung zustimmt. Entscheidend ist: Ein Beschäftigter muss regelmäßig eine wirksame Einwilligung zur Erhebung von (GPS-)Daten erklärt haben, um ihn orten zu dürfen. Insbesondere gilt, dass ein Arbeitgeber ein Smartphone nicht als Überwachungswerkzeug zur permanenten Leistungskontrolle für seine Mitarbeiter verwenden darf.

So wurde in einem Fall, in dem eine Detektei im Auftrag ein Bewegungsprofil eines Mitarbeiters mittels GPS-Sonde an dessen Fahrzeug erstellt hatte, eine Freiheitsstrafe von einem Jahr und sechs Monaten verhängt, ausgesetzt zur Bewährung (Landgericht Mannheim, Az. 4 KLs 408 Js 27973/08). Auch der Bundesgerichtshof musste sich mit diesem Thema auseinandersetzen und bestätigte die strafrechtliche Verurteilung im Wesentlichen (BGH, Az. 1 StR 32/13). Auch der Fall einer Supermarktkette sorgte für großes Aufsehen, da hier bestimmte Bereiche ohne Wissen und schriftliche Zustimmung der Mitarbeiter videoüberwacht wurden. Hier war es unter anderem das Ziel, vermeintliche Minderleister zu identifizieren und entsprechend zu maßregeln. Videoaufnahmen von Personen werden allerdings zweifellos ebenfalls als personenbezogene Daten

eingestuft. Ab dem 25. Mai 2018 gelten Bild- und Tonaufzeichnungen in den meisten Fällen sogar als biometrische Daten, für deren Verarbeitung besonders strenge Auflagen gelten werden. Die Erhebung dieser Daten im konkreten Fall war einem damaligen Urteil zu Folge nicht rechtens, da sie sich nicht auf einen bestimmten Einzelverdacht stützte und flächendeckend eingesetzt wurde – auch in Bereichen, in denen eine Überwachung grundsätzlich nicht zulässig ist.

Übrigens: Ein Mitarbeiter, der von seinem Vorgesetzten beauftragt wird, eine strafbare Handlung vorzunehmen (wie die GPS-Ortung eines anderen Mitarbeiters ohne dessen Wissen und Einverständnis), hat das Recht, die Befolgung dieser Anweisung zu verweigern. Er hat in einem solchen Fall keine arbeitsrechtlichen Konsequenzen zu befürchten. Seriöse Detekteien sollten entsprechende Aufträge von vornherein ablehnen.

Falls erforderlich, muss in jedem Einzelfall der Mitarbeiter informiert sein und schriftliches Einverständnis eingeholt werden, wenn von einem Mobilgerät ‚von außen' Daten erhoben werden. Anders verhält es sich, wenn ein Mitarbeiter um Erhebung dieser Daten bittet. Ein praktisches Beispiel wäre der Verlust des Gerätes und eine Bitte des Mitarbeiters, das Gerät zu orten. So kann auch sichergestellt werden, dass das Gerät nicht einfach nur verlegt wurde. Auch eine Fernlöschung auf Bitten des Mitarbeiters ist unproblematisch, wenn es sich um „sein" Gerät handelt. Unternehmenseigene Geräte können ebenfalls aus der Ferne gelöscht werden, sofern die Privatnutzung untersagt ist (s.o. „BYOD"). Aus praktischen Gründen sollte dies natürlich nur dann erfolgen, wenn der Mitarbeiter den Verlust eines Gerätes gemeldet hat bzw. darum gebeten hat.

7. Einsicht erlaubt?

Einsicht nehmen darf der Arbeitgeber grundsätzlich nur in geschäftliche Daten. Private Fotos, Nachrichten oder Emails sind tabu. Ein Arbeitgeber kann auf der Basis einer entsprechenden Vereinbarung jedoch von einem Beschäftigten verlangen, ein geschäftlich genutztes Privatgerät vorzuzeigen, um die Umsetzung von Auflagen sicherzustellen unter denen die geschäftliche Nutzung des Gerätes gestattet ist, wie zum Beispiel das Verschlüsseln des geräteinternen Speichers. Hierbei darf allerdings auch keine Einsicht in andere, potenziell private Daten genommen werden, auch „wenn man schon mal dabei ist und das Gerät sowieso gerade da hat". Ebenso kann der Arbeitgeber beim Ausscheiden eines Arbeitnehmers von ihm nicht die Herausgabe des Privatgerätes verlangen, um seinerseits geschäftliche Daten zu löschen.

Entscheidungen im Kontext MDM sollten verschriftlicht und in dieser Form den Mitarbeitern bekanntgemacht werden. Eine rechtlich saubere „Universallösung" ist allerdings nicht in Sicht, da die technischen und rechtlichen Rahmenbedingungen in den Unternehmen zu unterschiedlich sind. Aus diesem Grund ist es unabdingbar, sich für die Planung des Konzepts fachlichen Rats zu bedienen, den insbesondere Rechtsanwälte/innen, die sich auf IT- und Datenschutzrecht spezialisiert haben, beisteuern können.

8. Schlussbemerkung

Die vorstehenden Ausführungen dienen lediglich der Veranschaulichung möglicher Problemkonstellationen. Sie erheben keinen Anspruch auf Vollständigkeit und sind unverbindlich. Wir empfehlen jedem Unternehmen, sich entsprechend beraten zu lassen und - sofern vorhanden - frühzeitig den Datenschutzbeauftragen und den Betriebsrat zu involvieren.

Diese Publikation wurde mit freundlicher Unterstützung der SDS Rechtsanwälte Sander Dahm Schöning PartGmbB aus Duisburg (www.sds.ruhr) erstellt und stellt keinen Ersatz für eine umfassende und individuelle Rechtsberatung dar.

Rechtsanwälte
SANDER DAHM SCHÖNING
Partnerschaft mbB