Einsatz mobiler Endgeräte in Unternehmen

Einleitung

Datenschutzrechtliche Fragestellungen im Zusammenhang mit der Nutzung von mobilen Endgeräten in Unternehmen stellen sich in der aktuellen Situation verstärkt, da Arbeitnehmer angesichts der Kontaktbeschränkungen aufgrund der Corona-Pandemie auf Tele- und Videokommunikation angewiesen sind und dienstliche Tätigkeiten vermehrt in das Home Office ausgelagert werden. Diese Maßnahmen lassen sich häufig nur umsetzen, wenn die Mitarbeiter für ihre Tätigkeit mobile Endgeräte, beispielsweise Smartphones, Laptops und Tablets, nutzen können.

Bereits bei der Anschaffung und Einrichtung der Geräte, aber auch bei ihrer Nutzung durch die Arbeitnehmer sollte die Einhaltung datenschutzrechtlicher Bestimmungen sichergestellt werden. Wir haben dies zum Anlass genommen, das Thema vertieft aufzubereiten und möchten im Folgenden auf verschiedene datenschutzrechtliche Fragestellungen im Zusammenhang mit dem Einsatz mobiler Endgeräte in Unternehmen eingehen.

Das Risiko der Nutzung mobiler Endgeräte

Das datenschutzrechtliche Risiko bei der Nutzung mobiler Endgeräte wird gegenüber der Nutzung stationärer Geräte deswegen als erhöht angesehen, weil sie außerhalb des Unternehmens eingesetzt werden können. Dadurch steigt die Gefahr eines Verlustes oder Diebstahls des Geräts. Außerdem besteht das Risiko einer unbefugten Datenübermittlung, etwa an das heimische Netzwerk des Mitarbeiters. Der Arbeitgeber hat bei der Nutzung des mobilen Endgeräts außerhalb des Unternehmens nur eingeschränkten Einfluss darauf, ob der Mitarbeiter tatsächlich in einer Umgebung tätig ist, in der die Vertraulichkeit der Daten gewahrt ist. Dies kann von ihm auch nur eingeschränkt überprüft werden.

Um trotz dieser Risiken von den Vorteilen der Nutzung mobiler Endgeräte profitieren zu können und gleichzeitig den Schutz personenbezogener Daten zu gewährleisten, sind angemessene Schutzmaßnahmen zu treffen.

Auswahl und Beschaffung mobiler Endgeräte, Nutzung privater Geräte

Bereits bei der Auswahl und Beschaffung von mobilen Endgeräten sollten neben den funktionalen Bedürfnissen der Nutzer auch Aspekte des Datenschutzes berücksichtigt werden. Insbesondere sollten die integrierten Sicherheitsvorkehrungen des Geräts und der Betriebssoftware einen angemessenen Schutz ermöglichen. Auch auf die Vertrauenswürdigkeit von Lieferanten und Herstellern ist zu achten.

Im Zusammenhang mit der Auswahl und Beschaffung mobiler Endgeräte stellt sich regelmäßig die Frage, ob Arbeitnehmer für ihre dienstliche Tätigkeit ihre eigenen privaten Geräte benutzen dürfen („Bring Your Own Device", „BYOD"). Vorteile davon werden in der Ersparnis von Anschaffungs- und Unterhaltskosten gesehen. Außerdem könne sich die Produktivität der Arbeitnehmer vor allem bei alltäglichen Prozessen wie der E-Mail- oder Terminverwaltung verbessern.

Bei der Nutzung privater Geräte stellen sich aber auch einige datenschutzrechtliche Probleme. Für Unternehmen ist es schwieriger, auf privaten Geräten ausreichende Sicherheitsmaßnahmen zu gewährleisten. Da auf den Geräten sowohl dienstliche als auch private Daten vorhanden sind, der Arbeitgeber in der Regel aber nur für die Einsicht in dienstliche Daten eine Rechtsgrundlage haben wird, sind Kontrollen der privaten Geräte durch den Arbeitgeber schwieriger umsetzbar.

Die Nutzung von privaten Geräten für dienstliche Tätigkeiten ist daher grundsätzlich nicht zu empfehlen. Dies gilt insbesondere, soweit personenbezogene Daten und andere besonders schützenswerte dienstliche Daten auf dem Gerät verarbeitet werden sollen.

Eine Nutzung privater Geräte kann allenfalls dann datenschutzkonform möglich sein, wenn dabei sichergestellt wird, dass das in dem Unternehmen festgelegte Datenschutzniveau nicht unterschritten wird. Die Geräte sollten möglichst die gleichen Sicherheitsanforderungen erfüllen, die auch Dienstgeräte erfüllen müssen. Personenbezogene Daten des Unternehmens sollten nicht auf dem Privatgerät selbst verarbeitet werden. Sie sollten nicht aus dem Unternehmensnetzwerk auf das private Gerät, von dem aus der Zugriff erfolgt, übertragen werden können.

Angesichts der Corona-Pandemie hat der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) auf seiner Internetseite über die dienstliche Nutzung von Privatgeräten informiert. Elektronische Kommunikation sei derzeit in einem größeren Umfang zwingend erforderlich. Da es für die öffentlichen Stellen schwierig sei, hierfür dienstliche Geräte zur Verfügung zu stellen, akzeptiere der Bayerische Landesdatenschutzbeauftragte vorübergehend und unter bestimmten Voraussetzungen die Verwendung von Privatgeräten. Dies soll für Videokonferenzen und Messengerdienste zur Kommunikation von Beschäftigten in öffentlichen Stellen untereinander sowie mit externen Personen gelten. Voraussetzung sei, dass gewisse Sicherheitsvorkehrungen getroffen werden, indem etwa die Kommunikation möglichst datensparsam erfolgt, sensible Daten nicht auf dem Privatgerät gespeichert werden und die Geräte passwortgeschützt sind. Die-

ser Position hat sich auch die Landesbeauftragte für den Datenschutz Niedersachsen angeschlossen.

Technische und organisatorische Maßnahmen

Verantwortliche Stellen und ihre Auftragsverarbeiter haben nach Art. 32 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten.

Im Zusammenhang mit der Umsetzung von technischen und organisatorischen Maßnahmen spielen die Grundsätze „Privacy by Design" und „Privacy by Default" eine Rolle. Diese Grundsätze sollten bereits bei der Einrichtung mobiler Endgeräte beachtet werden. Der Grundsatz „Privacy by Design" („Datenschutz durch Technikgestaltung") besagt, dass Datenschutzmaßnahmen bereits bei der Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert sein sollten. Der Grundsatz „Privacy by Default" („Datenschutz durch datenschutzfreundliche Voreinstellungen") aus Art. 25 Abs. 2 S. 1 DSGVO bedeutet, dass bereits durch die Voreinstellungen nur personenbezogene Daten verarbeitet werden sollen, die für den konkreten Verarbeitungszweck erforderlich sind. Dazu gehört auch, dass jeder Mitarbeiter aufgrund der Berechtigungsstrukturen auf dem Gerät nur auf die Daten zugreifen kann, die er für seine dienstliche Tätigkeit benötigt.

Technisch kann es empfehlenswert sein, das mobile Gerät nur als Zugangsmöglichkeit zu den Servern des Unternehmens zu verwenden, sodass etwa über eine VPN-Verbindung auf den Servern des Unternehmens gearbeitet wird und auf dem mobilen Gerät keine Daten abgelegt werden. Das Gerät sollte zudem mittels eines Passwortes beziehungsweise einer PIN geschützt sein. Einem Datenverlust bei einem Diebstahl können außerdem die Sicherung von Laptops durch ein Schloss sowie Verschlüsselungstechniken entgegenwirken. Der Verlust des Gerätes führt dann nicht unweigerlich zum Verlust der Datenvertraulichkeit. Vor diesem Hintergrund sind auch zentrale Löschmöglichkeiten per Fernzugriff für die Daten auf den Mobilgeräten zu empfehlen. Weitere Schutzmaßnahmen sind die Installation von Virenschutzsoftware sowie die Durchführung von Sicherheitsupdates und Datensicherungen.

Zu den organisatorischen Maßnahmen gehört die Sensibilisierung der Mitarbeiter. Unternehmen ist zu raten, in Bezug auf die Nutzung mobiler Endgeräte klare Regelungen zu formulieren, damit Mitarbeiter die erforderlichen Schutzmaßnahmen leichter umsetzen können. Anweisungen an die Mitarbeiter können etwa die Nutzung privater Geräte und das Verbot einer Weitergabe des Geräts an Dritte betreffen. Um einen ungewollten Datenaustausch zu verhindern, kann durch entsprechende Anweisungen auch die Verbindung des Geräts mit unbekannten Netzen, offenen WLANs und Hotspots verboten werden.

Nutzung der mobilen Endgeräte durch Mitarbeiter

Nach der Anschaffung und Einrichtung des mobilen Endgeräts stellen sich auch bei dessen Nutzung durch den Arbeitnehmer datenschutzrechtliche Fragen. Einige typische Konstellationen sollen im Zusammenhang mit konkret zu treffenden Schutzmaßnahmen im Folgenden näher dargestellt werden.

Home Office

Bei der Tätigkeit an Heimarbeitsplätzen kommen regelmäßig mobile Endgeräte zum Einsatz. Besonders in der aktuellen Situation angesichts der Corona-Pandemie werden verstärkt Tätigkeiten in das Home Office ausgelagert. Über die Auslagerung von Tätigkeiten in das Home Office im Zusammenhang mit der Corona-Pandemie haben wir bereits in unserem Newsletter im April 2020 berichtet.

Auch bei der Tätigkeit im Home Office gilt, dass das allgemein im Unternehmen festgelegte Datenschutzniveau nicht unterschritten werden sollte. Dies kann dadurch abgesichert werden, dass der Arbeitgeber durch Anweisungen die Rahmenbedingungen für diese Form der Tätigkeit vorgibt. In diesem Zusammenhang können die technischen Voraussetzungen des Einsatzes mobiler Endgeräte im Home Office festgelegt werden, wonach die Mitarbeiter beispielsweise nur über dienstliche Geräte mittels eines VPN-Zugangs auf dienstliche Daten zugreifen dürfen. Die Mitarbeiter sollten auch darauf hingewiesen werden, dass die Geräte vor dem unberechtigten Zugriff Dritter, einschließlich etwaiger Familienangehöriger und sonstiger Mitbewohner, zu schützen sind, indem sie etwa in einem separaten Raum aufgebaut werden und bei Inaktivität des Nutzers ein Bildschirmschoner aktiviert wird.

Private Nutzung

Wenn dienstliche Geräte von einem Unternehmen zur Verfügung gestellt werden, stellt sich die Frage, ob Arbeitnehmer diese auch privat nutzen dürfen. In diesem Zusammenhang können sich datenschutzrechtliche Probleme ergeben. Bei der Wartung des Geräts etwa sollten von dem Unternehmen nicht private Daten des Arbeitnehmers verarbeitet werden. Diese sollten auch von einer betrieblichen Datensicherung nicht umfasst sein. Umgekehrt muss ausgeschlossen sein, das privat genutzte Online-Dienste und Apps, wie zum Beispiel soziale Netzwerke, auf die dienstlichen Daten zugreifen können. Dienstliche und private Anwendungen und Daten sollten auf dem Gerät im Idealfall voneinander getrennt sein. Nur wenn eine unberechtigte Verarbeitung von privaten Daten durch das Unternehmen sowie ein Zugriff von privaten Anwendungen auf dienstliche Daten ausgeschlossen werden können, kann die private Nutzung dienstlicher Geräte datenschutzkonform erlaubt werden.

Durchführung von Updates und Installation von Software durch Mitarbeiter

In einem Unternehmen sollte es zudem klare Vorgaben geben, ob und inwieweit Installationen und Updates auf den Geräten von den Mitarbeitern selbst vorgenommen werden dürfen. Um ein einheitliches Datenschutzniveau zu gewährleisten, kann es empfehlenswert sein, die Sicherheitseinstellungen auf den Geräten möglichst zentral zu konfigurieren. Durch die Etablierung eines Autorisierungssystems für die Installation von Software kann es beispielsweise nur dem Administrator aus der IT-Abteilung erlaubt werden, Installationen vorzunehmen. Zudem kann es hilfreich sein, eine Liste mit Programmen und Apps, die auf mobilen Endgeräten installiert werden dürfen, bereitzuhalten.

Nutzung von WhatsApp

Über den Einsatz von WhatsApp in Unternehmen haben wir in unserem Newsletter im März 2018 ausführlich informiert. Datenschutzrechtlich problematisch ist dabei, dass durch die Installation von WhatsApp der Nutzer der App typischerweise die Berechtigung erteilt, die Kontaktdaten des eingesetzten Mobilgeräts auszulesen. Die in dem Adressbuch gespeicherten Daten werden dann in regelmäßigen Abständen an die Server von WhatsApp übermittelt, was regelmäßig ohne Einwilligung der gespeicherten Kontakte und insoweit ohne Rechtsgrundlage geschieht.

Für die datenschutzrechtliche Beurteilung sind unterschiedliche Konstellationen zu unterscheiden: In einem Fall soll WhatsApp auf dienstlichen Mobilgeräten installiert werden. In einem anderen Fall wird WhatsApp auf privaten Geräten der Mitarbeiter verwendet, die auch für dienstliche Zwecke genutzt werden.

Auf Dienstgeräten kann durch ein generelles Verbot der Installation von WhatsApp verhindert werden, dass eine Datenübermittlung an WhatsApp stattfindet. Alternativ ist es möglich, den Einsatz von WhatsApp zu erlauben, aber dafür die Nutzung des Adressbuchs auf dem Mobilgerät zu verbieten. Soweit in dem Adressbuch keine personenbezogenen Daten gespeichert sind, werden von dort auch keine Daten an WhatsApp übermittelt. Eine dritte Möglichkeit ist es, WhatsApp den Zugriff auf das Adressbuch zu verweigern, indem das Adressbuch in einen isolierten Bereich des Mobilgeräts, eine sogenannte „Sandbox", ausgegliedert wird. Der Zugriff auf das Adressbuch kann WhatsApp außerdem über das Rechtemanagement in den Einstellungen des Mobilgeräts verweigert werden. Es ist dabei aber darauf zu achten, dass diese Einstellung von Beginn an und dauerhaft für WhatsApp gilt.

In den Fällen, in denen Mitarbeiter ihre Privatgeräte für dienstliche Zwecke nutzen dürfen, kann ebenfalls eine Übermittlung von gespeicherten dienstlichen Kontaktdaten an WhatsApp drohen. Ein Verbot der Nutzung bestimmter Applikationen ist auf Privatgeräten regelmäßig nur schwer durchsetzbar. Stattdessen sollte etwa durch Weisungen an die Mitarbeiter sichergestellt werden, dass keine dienstlichen Kontaktdaten auf dem privaten Gerät gespeichert werden. Der Einsatz von Mobile Device Management-Systemen kann für die Abgrenzung der privaten und dienstlichen Bereiche auf dem Gerät sorgen. Soweit hierdurch sichergestellt ist, dass die dienstlichen Kontakte nicht über das Adressbuch synchronisiert und an WhatsApp übermittelt werden, besteht zwischen der privaten Nutzung einschließlich WhatsApp und der dienstlichen Nutzung in einem abgeschotteten Bereich kein Konflikt.

Diese Ausführungen gelten entsprechend auch für andere Anwendungen, soweit mit deren Nutzung ebenfalls eine Datenübermittlung an externe Unternehmen verbunden ist und sich insoweit ähnliche datenschutzrechtliche Probleme stellen.

Datenschutzvorfälle

Durch den Verlust oder den Diebstahl mobiler Endgeräte kann es zu Verletzungen des Schutzes personenbezogener Daten kommen. Solche Verletzungen müssen nach Art. 33, 34 DSGVO der Aufsichtsbehörde und dem Betroffenen gemeldet werden, soweit die Verletzung voraussichtlich zu einem Risiko beziehungsweise zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Durch klare Anweisungen im Vorfeld und strukturierte vorgegebene Arbeitsabläufe ist den Mitarbeitern des Unternehmens eine schnelle Reaktion auf Datenschutzverletzungen möglich. Auf diese Weise kann auch die Einhaltung der kurzen Frist für Meldungen an die Aufsichtsbehörde, die möglichst innerhalb von 72 Stunden zu erfolgen haben, eingehalten werden.

Mitarbeiter sollten den Verlust ihres mobilen Endgeräts unverzüglich dem Arbeitgeber melden, damit Schutzmaßnahmen getroffen werden können. Diese beinhalten beispielsweise die Löschung der personenbezogenen Daten von dem Gerät aus der Ferne, um eine unbefugte Verarbeitung der Daten zu verhindern.

Fazit

Unternehmen sollten sich bei dem Einsatz von mobilen Endgeräten frühzeitig mit den damit zusammenhängenden datenschutzrechtlichen Fragestellungen beschäftigen. Durch angemessene Schutzmaßnahmen sollte sichergestellt werden, dass das allgemein im Unternehmen festgelegte Datenschutzniveau auch bei der Nutzung mobiler Geräte nicht unterschritten wird. Es ist empfehlenswert, datenschutzrechtliche Aspekte im Zusammenhang mit dem Einsatz von mobilen Endgeräten im Unternehmen vorab zu regeln und zu dokumentieren. Dies kann etwa durch konkrete Vorgaben für einzelne Fälle, beispielsweise für die Auslagerung von Tätigkeiten in das Home Office, aber auch durch die Zusammenfassung aller Weisungen und Empfehlungen an die Mitarbeiter, die einen Bezug zu der Nutzung der betrieblichen IT-Systeme aufweisen, im Rahmen einer einheitlichen IT-Richtlinie geschehen..

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin
T +49 521 96535 - 890
F +49 521 96535 - 114
M johanna.schmale@brandi.net
www.brandi.net