MATERNA
Virtual Solution

BYOD-Modelle rechtlich absichern

Was Unternehmen & Behörden unbedingt wissen sollten

Materna Virtual Solution GmbH · Juni 2022

MATERNA Virtual Solution

BYOD-Modell? So stellen Sie es rechtlich auf sichere Beine!

Bring your own device, kurz: BYOD, bezeichnet die Nutzung von privaten Endgeräten für berufliche bzw. dienstliche Zwecke. Dies umfasst den beruflichen Einsatz sowohl privater Hardware wie z. B. Smartphones als auch kommerzieller und privater Software, wie bspw. WhatsApp. BYOD beschreibt einerseits das Verhalten der Nutzer:innen, andererseits aber auch eine organisatorische Strategie. Es hat für Arbeitnehmende und Arbeitgebende viele Vorteile. Es ergeben sich jedoch automatisch auch einige rechtliche Aspekte, die es zu beachten gilt.

Nach dem Lesen dieses Whitepapers kennen Sie

- Wichtige technische & organisatorische Regelungen für den BYOD-Einsatz
- Arbeitsrechtliche Aspekte, die bei BYOD zu beachten sind
- Alle internen Abteilungen, die Sie vor der BYOD-Einführung hinzuziehen müssen
- Das nötige Vertragswerk für eine Abdeckung der rechtlichen Aspekte
- Lösungsansätze für sichere BYOD-Modelle

MATERNA Virtual Solution

Inhalt

Seite

BYOD einführen – diese Rechtsbereiche sind betroffen

Bei der Einführung von BYOD-Modellen sind gleich mehrere Rechtsaspekte zu berücksichtigen. Insbesondere dann, wenn Mitarbeitende private Endgeräte für berufliche Zwecke nutzen und damit auf das Unternehmensnetzwerk zugreifen können. Die wesentlichen rechtlichen Themen wie etwa Datenschutz, IT-Sicherheit und Arbeitsrecht stellen wir Ihnen hier kurz vor, damit Sie sich vorab optimal informieren und strategisch entsprechend planen können.

DSGVO: Was es beim Datenschutz zu beachten gibt

Bei der Erstellung und Verwaltung von E-Mails und Dokumenten verarbeiten die Beschäftigten für Arbeitgebende immer auch so genannte personenbezogene Daten. Damit sind *»alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person* (betroffene Person) *beziehen«*, gemeint.

Nach der Datenschutzgrundverordnung (DSGVO) wird als identifizierbar *»eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann«* (Art. 4 Nr. 1 DSGVO).

MATERNA Virtual Solution

Verantwortlichkeiten der Arbeitgebenden

Arbeitgebende bzw. Behörden sind sogenannte »Verantwortliche« im Sinne von Art. 4 Nr. 7 DSGVO, denn er bzw. sie entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten. Das heißt, er bzw. sie ist verantwortlich für die Einhaltung des Datenschutzes in Bezug auf die personenbezogenen Daten, die im Unternehmen bzw. der Behörde verarbeitet werden (z. B. Kunden- oder Mitarbeiter:innendaten). Arbeitgebende bzw. Behörden bleiben die verantwortliche Stelle. Auch dann, wenn die Beschäftigten die Daten im Zuge eines BYOD-Modells auf ihren privaten Geräten verarbeiten. Arbeitgebende sind dafür verantwortlich, dass ausreichende technische und organisatorische Maßnahmen (sogenannte TOMs, vgl. Art. 32 DSGVO) getroffen werden.

Gemäß Art. 32 Abs. 1 DSGVO müssen die von den Verantwortlichen und den Auftragsverarbeitenden getroffenen TOMs *»unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen«* geeignet sein, *»um ein dem Risiko angemessenes Schutzniveau zu gewährleisten«.*

Was bedeutet das? Die Verantwortlichen müssen dafür Sorge tragen, dass die personenbezogenen Daten auf dem Gerät der Beschäftigten so sicher sind, wie sie es auch auf der unternehmen- bzw. behördeneigenen IT-Infrastruktur wären.

Die Sicherheit der Daten lässt sich u. a. durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren gewährleisten (siehe Art. 32 Abs. 1 lit. a) DSGVO).

Datenschutz »by design and by default«

Bei einem BYOD-Modell wie auch bei der Nutzung privater Endgeräte im Homeoffice gehen die datenschutzrechtlichen Aufsichtsbehörden[1] davon aus, dass die Daten des Unternehmens in einem verschlüsselten Bereich gesondert gespeichert sind. Zudem sind berufliche von privaten Daten strikt zu trennen. Arbeitgebende müssen außerdem die Möglichkeit haben, ihre Daten – auch aus der Ferne – zu löschen. Die DSGVO sieht vor, dass der Datenschutz bereits bei der Entwicklung neuer Produkte einbezogen ist und dass grundsätzlich mit datenschutzfreundlichen Voreinstellungen gearbeitet wird (»Data protection by design and by default«, Art. 25 DSGVO). Beides Anforderungen, die auch für BYOD eine wichtige Rolle spielen.

Aufsichtsbehörden können bei Verstößen Bußgelder von bis zu 20 Millionen Euro oder von bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes verhängen.

Gemäß Art. 83 Abs. 4 DSGVO können die Aufsichtsbehörden Bußgelder von bis zu 20 Millionen Euro oder von bis zu 4 Prozent[2] des gesamten weltweit erzielten Jahresumsatzes verhängen. Keine schöne Vorstellung. Es lohnt sich, den Gesetzestext noch genauer zu betrachten: Aufgrund der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO gilt dies schon dann, wenn die TOMs nur nicht dokumentiert sind. Warum?

Die Verantwortlichen sind für die Rechtmäßigkeit der Datenverarbeitung und die Integrität und Vertraulichkeit der personenbezogenen Daten verantwortlich. Sie sind es, die die Einhaltung nachzuweisen haben, auch ohne dass es erst zu einem Datenschutzverstoß gekommen sein muss. Sind wirksame TOMs umgesetzt und dokumentiert, die sogar über das übliche Maß hinausgehen, kann dies bei der Bemessung der Bußgeldhöhe nach DSGVO positiv zugunsten der Verantwortlichen gewertet werden (vgl. Art. 83 Abs. 2 lit. d) DSGVO).

Unternehmenswerte sichern: Geheimnisschutz

Mobile Endgeräte sind einer Vielzahl von potenziellen Bedrohungen ausgesetzt[3]. Bereits aufgrund der Größe und der Mobilität ist das Risiko des Geräteverlusts bzw. des Diebstahls erhöht. Die Möglichkeit der Fernlöschung dient daher u. a. auch dazu, sicherzustellen, dass Geschäftsgeheimnisse des Unternehmens im Sinne von § 2 Nr. 1 des Geschäftsgeheimnisgesetzes nicht in die Hände von Unbefugten gelangen können. Es verlangt nämlich, dass Geschäftsgeheimnisse *»Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber«* sind. Um firmeninternes Know-how zu schützen, muss das Unternehmen angemessene IT-Sicherheitsmaßnahmen implementiert haben. Dazu zählen zum Beispiel die Verschlüsselung elektronischer Dokumente und die Verhinderung des Zugriffs ohne Authentifizierung. Zusätzliche Sicherheit bietet die Ende-zu-Ende-Verschlüsselung von E-Mails und angehängter Dokumente. Sie macht ein »Mitlesen« durch Dritte nahezu unmöglich.

Datenlecks sind zu schließen, denn ein in Kauf genommenes Leck kann zu der Bewertung führen, dass insgesamt kein angemessenes Schutzniveau mehr vorliegt und somit auch kein Geheimnisschutz.[4]

1 Vgl. »Hilfestellung zum Datenschutz im Homeoffice« (Stand: Juli 2020) der Landesbeauftragten für den Datenschutz Niedersachsen.
2 https://dsgvo-gesetz.de/themen/bussgelder-strafen/
3 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI), Broschüre »Sicheres mobiles Arbeiten«.
4 OLG Stuttgart, Urteil vom 19.11.2020, Az. 2 U 575/19.

MATERNA Virtual Solution

Was, wenn das Gerät samt gespeicherter Dokumente gestohlen wird, verloren geht oder Mitarbeiter:innen ausscheiden? Bei sicheren Kommunikationsanwendungen lassen sich die Geschäftsdaten in einem verschlüsselten Bereich, dem so genannten Container, schnell »remote« löschen. Alle anderen privaten Apps und Daten bleiben vollständig erhalten.

Wo Arbeitgebende ohne eigenes Verschulden haften: Urheberrechtsschutz

Gemäß § 99 Urheberrechtsgesetz (UrhG) ist das Unternehmen eigenständig und verschuldensunabhängig verantwortlich, wenn Arbeitnehmende ein Urheberrecht verletzen. Dies könnte z. B. dadurch verletzt werden, dass ein(e) Arbeitnehmer:in im Rahmen des BYOD-Modells eine Software beruflich einsetzt, die er bzw. sie privat erworben hat. Diese wäre damit nur für die private Nutzung lizenziert, z. B. weil er/sie die Nutzung dieser Software für intuitiver hält als die Unternehmenssoftware.

Trotzdem wäre das Unternehmen oder auch das Organ, d. h. die Geschäftsführung oder der Vorstand, im Rahmen der Organhaftung (§ 43 GmbHG bzw. §§ 91 Abs. 2, 93 AktG) persönlich hierfür haftbar. Und zwar dann, wenn nicht sichergestellt ist, dass ernsthafte und geeignete Schutzvorkehrungen getroffen worden sind, um Urheberrechtsverletzungen zu verhindern.

Trotzdem wäre das Unternehmen oder auch … die Geschäftsführenden oder Vorständ:innen … persönlich hierfür haftbar.

Berufliche Kommunikation: Aufbewahrungspflichten

Die gesetzlichen Aufbewahrungspflichten z. B. gemäß § 257 HGB und § 147 AO sowie gemäß den »Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« (GoBD) sind einzuhalten. Sämtliche berufliche Kommunikation muss über den beruflichen E-Mail-Account geführt werden, um zu verhindern, dass geschäftsrelevante Kommunikation an Verantwortlichen vorbeiläuft und nicht zentral gespeichert wird.

BYOD-Modelle rechtlich absichern: ein Lösungsansatz

Die genannten rechtlichen Anforderungen (v. a. Datentrennung, Verschlüsselung, Fernlöschung, Unterbinden von Copy-and-Paste, zentrale Aufbewahrung) kann eine spezielle Anwendungssoftware (App) erfüllen. Die Container-Technologie trennt dabei die privaten von den beruflichen bzw. dienstlichen Daten. Zum Öffnen der App müssen die Nutzer:innen eine zusätzliche, vom Gerätepasswort unabhängige Authentifizierung durchführen, sodass Dritte keinen Zugriff auf die Daten nehmen können.

BYOD-Einsatz auch mit den Beschäftigten klar regeln

Im Rahmen eines BYOD-Modells müssen einige weitere Punkte geregelt sein, die nur durch eine zusätzliche Vereinbarung mit den Beschäftigten und ggf. einer Betriebsvereinbarung mit dem Betriebs-/Personalrat abgedeckt werden können. Dies ist umso wichtiger, weil es zu BYOD weder spezifische Regelungen in Gesetzen gibt, noch bislang eine detaillierte Rechtsprechung zu dem Thema ergangen ist.

Sicherheit der Daten

Hierbei sind u. a. Richtlinien oder technische Dokumentationen für das BYOD-Modell zu nennen, die für die Teilnehmer:innen daran verbindlich und für die Sicherheit der Daten wichtig sind: Beschäftigte verpflichten sich, immer ein aktuelles Betriebssystem sowie einen aktuellen Virenschutz einzusetzen, das eigene Gerät nicht zu »jailbreaken« bzw. zu »rooten« – d. h. die Nutzungsbeschränkungen des Herstellers nicht zu umgehen –, das Gerät nicht an Dritte weiterzugeben, private Daten selbst zu sichern.

Darüber hinaus ist zu regeln, in welchen Fällen eine (kurzzeitige) Herausgabe des Gerätes von den Beschäftigten verlangt werden darf. Für die Sicherheit der Daten sind zudem Regelungen zur Beendigung der Teilnahme am BYOD-Modell (auch durch Beendigung des Arbeitsverhältnisses) zu treffen.

Was Beschäftigte wissen müssen: Mitteilungspflichten

Wichtig ist es zudem, den Beschäftigten Mitteilungspflichten aufzuerlegen, z. B. bei Verlust/Diebstahl des Gerätes, damit zeitnah eine Fernlöschung durchgeführt werden kann. Es sollte auch sichergestellt sein, dass etwaige Meldepflichten des Unternehmens nach Art. 33 DSGVO erfüllt werden können, wenn eine Verletzung des Schutzes personenbezogener Daten erfolgt. Etwa weil Daten unrechtmäßig übermittelt wurden oder Dritte unbefugten Zugang zu personenbezogenen Daten erlangt haben. Die Meldepflicht gilt nicht nur bei Datenpannen hinsichtlich »sensibler« Daten, sondern bei jeglicher Verletzung des Schutzes personenbezogener Daten. Also z. B. auch bei einem bloßen Datenverlust, ohne dass es einer unrechtmäßigen Kenntnisnahme durch Dritte bedarf. Die Meldepflicht stellt bei einer solchen Verletzung den Regelfall dar. Verantwortliche müssen es nur dann nicht melden, wenn *»die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt«*. Zudem ist nach Art. 33 DSGVO unverzüglich Meldung zu machen, möglichst innerhalb von 72 Stunden.

MATERNA Virtual Solution

Neben der Meldepflicht gegenüber der Aufsichtsbehörde besteht nach Art. 34 DSGVO die Pflicht, die von der Datenpanne betroffenen Personen zu benachrichtigen, wenn *»die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge«* hat. Diese Benachrichtigung ist aber dann nicht erforderlich, wenn *»der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung«* (Art. 34 Abs. 3 lit. a) DSGVO).

Was bedeutet das für Sie als Verantwortliche:r?

Sind personenbezogene Daten durch eine spezielle Anwendungssoftware wie z. B. SecurePIM verschlüsselt, lassen sich die hohen Kosten, die durch solch eine Benachrichtigung der Betroffenen entstehen und der daraus resultierende Imageschaden vermeiden.

Wirklich alles bedacht?

Die Beschäftigten haben das Endgerät, das im Rahmen des BYOD-Modells beruflich zum Einsatz kommen soll entweder von einem Händler erworben oder bekommen es von ihrem Mobilfunkanbieter während der Vertragslaufzeit zur Verfügung gestellt. Und nachdem das Eigentum weiterhin beim Beschäftigten verbleiben soll, stellen sich noch folgende Fragen:

Aus dem Vertragsrecht

»Wer ist für Wartung oder Reparatur verantwortlich? Erlaubt der Vertrag des Beschäftigten nur die private Nutzung oder ist auch die Nutzung für berufliche Zwecke zulässig?«

Aus dem Steuerrecht

»Wie werden unsere Mitarbeiter:innen für die Nutzung ihrer privaten Geräte entschädigt? Beteiligen wir uns an den Kosten ihres Mobilfunkvertrages oder wird der Mobilfunkvertrag des Unternehmens genutzt? Ist hierbei eventuell ein geldwerter Vorteil zu versteuern?«

Aus dem Haftungsrecht

»Wer haftet eigentlich bei Verlust oder Beschädigung des Gerätes während der beruflichen Tätigkeit? Für BYOD-Modelle existiert ja noch keine detaillierte Rechtsprechung. Dann greift § 670 BGB analog, wonach ein Erstattungsanspruch gegen die Arbeitgebenden in Betracht kommt. Wir sollten also als Unternehmen eine Versicherung für das Gerät abschließen.«

MATERNA Virtual Solution

Das Arbeitsrecht im Blick haben!

Genauso, wie wenn die Beschäftigten ein berufliches Endgerät zur Verfügung gestellt bekommen würden, stellen sich außerdem arbeitsrechtliche Fragen, die teilweise gerichtlich noch nicht abschließend geklärt sind. Hierzu gehört vor allem die Frage, wie damit umzugehen ist, dass die Beschäftigten grundsätzlich permanent erreichbar sind (gerade bei der Nutzung eines privaten Gerätes), gleichzeitig aber die vereinbarte Arbeitszeit nicht überschritten werden darf und auch das Arbeitszeitgesetz (ArbZG) vor allem im Hinblick auf Ruhezeiten, eingehalten werden muss. Hierbei wird auch zu unterscheiden sein, ob die Beschäftigten außerhalb der regulären »Kern-«Arbeitszeit freiwillige Tätigkeiten entfalten oder ob sie hierzu angewiesen werden. Hierfür sind klare und verlässliche Regelungen vorzusehen.

Empfehlung: Arbeitnehmervertretung einbeziehen

Wenn im Unternehmen ein Betriebs-/Personalrat besteht, so muss dieser schon in der Planungsphase einbezogen und informiert werden (vgl. § 90 Abs. 1 Betriebsverfassungsgesetz (BetrVG)). Zwar kann das Gremium nicht über das private Eigentum der Beschäftigten bestimmen, wohl aber über die Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb (§ 87 Abs. 1 Nr. 1 BetrVG), über Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen sowie Verteilung der Arbeitszeit auf die einzelnen Wochentage (§ 87 Abs. 1 Nr. 2 BetrVG) und über die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG).

Doch mit funktionierenden Infrastrukturen und Technologien ist es nicht getan. Auch in den Köpfen muss sich einiges bewegen.

Sonderfall: Mobile-Device-Management-System

Entscheidet sich das Unternehmen dafür, im Rahmen des BYOD Modells ein sog. Mobile-Device-Management-System (MDM) zusätzlich zur Container-Lösung wie z.B. SecurePIM, einzusetzen, werden hierdurch weitreichende Möglichkeiten für Zugriffe und Einsichtnahmen im Unternehmen geschaffen. Dazu müssen Beschäftigte zusätzlich einwilligen. Andernfalls käme z. B. eine Strafbarkeit gemäß § 202a Strafgesetzbuch (StGB) (»Ausspähen von Daten«), gemäß § 202b StGB (»Abfangen von Daten«), § 202c StGB (»Vorbereiten des Ausspähens und Abfangens von Daten«) oder auch § 303a StGB (»Datenveränderung«) in Betracht.

Es stellen sich auch Fragen hinsichtlich des Schutzes der Privatsphäre der Beschäftigten – vor allem des Rechtes auf informationelle Selbstbestimmung, Art. 2 Abs. 1 in Verbindung mit Art. 1 Grundgesetz, GG – sowie Fragen hinsichtlich der Verletzung des Fernmeldegeheimnisses (§ 88 Telekommunikationsgesetz, TKG, ab dem 1. Dezember 2021 § 3 Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG), wenn die Arbeitgebenden eventuell Zugriff auf private E-Mails nehmen oder das private Surfverhalten überwachen können. Es ist dabei fraglich, ob es der Akzeptanz eines BYOD-Modells zuträglich ist, wenn sich die Beschäftigten ggf. von Arbeitgebenden »beobachtet« fühlen, sodass eine Lösung ohne die Zuhilfenahme eines MDM-Systems vorzugswürdig scheint.

Quick-Check 1: Relevante Abteilungen

Sie möchten ein BYOD-Modell in Ihrem Unternehmen oder in Ihrer Behörde einführen? Wunderbar! Hier folgt eine kurze Checkliste mit allen Abteilungen und Stellen, die Sie vor und während der Einführung hinzuziehen sollten:

- **IT-Abteilung**
  Zur Abklärung technischer Details, vor allem für die Installation der Anwendungssoftware bzw. für den Installations-Selfservice für die Beschäftigten. Strategisch bedenken: Durch die Heterogenität der privaten Geräte ergibt sich für die IT ggf. ein höherer administrativer Aufwand.

- **IT-Sicherheitsbeauftragte/r**
  Der oder die IT-Sicherheitsbeauftragte kann in einem Unternehmen oder einer Behörde für das Steuern und Koordinieren des IT-Sicherheitsprozesses zuständig sein und ist dann zusätzlich zur IT-Abteilung einzubeziehen.

- **Personalabteilung**
  HR ist zuständig für zu unterzeichnende Vereinbarungen der Mitarbeiter:innen bzgl. BYOD-Szenarien und zur Verwahrung dieser Dokumente in der Personalakte.

- **Betriebs- und Personalrat**
  Falls diese Gremien im Unternehmen bestehen, sind sie von Anfang an in das Projekt einzubeziehen (§ 87 Abs. 1 Nr. 1, 2, 6 BetrVG).

- **Rechtsabteilung**
  Sie muss die Vereinbarung für Mitarbeiter:innen erstellen und ggf. mit den Betriebs- bzw. Personalrät:innen verhandeln.

- **Datenschutzbeauftragte/r**
  Sie sind bei der Verarbeitung personenbezogener Daten immer einzubinden. Frühzeitige Information über die BYOD-Einführung und das zugrunde liegende Vertragswerk ist also erforderlich.

Quick-Check 2: Wesentliche Dokumente

Die betreffenden Abteilungen haben Sie eingebunden. Nun brauchen Sie noch das nötige Vertragswerk für eine rechtssichere Einführung. Hier eine kurze Übersicht über die relevanten Dokumente:

- **Technische Dokumentation mit Freigabeformular**
  Hier sollte geregelt sein, mit welchem Gerät Beschäftigte jeweils am BYOD-Modell teilnehmen dürfen. Die Dokumentation hält fest, welche Mindestanforderungen an Hardware und Betriebssystem bestehen, welche Apps installiert werden dürfen, wie die Installation abläuft und wer die Teilnahme genehmigt hat. Nicht zu vergessen: Sie sollten die technischen und organisatorischen Maßnahmen des BYOD-Modells regeln, wie beispielsweise Passwortrichtlinien, Verschlüsselung, klare Trennung von privaten und betrieblichen Daten, Patch- und Updatemanagement sowie aktueller Virenschutz.

- **Betriebsvereinbarung**
  Wenn ein Betriebs- bzw. Personalrat besteht, ist sie notwendig. Hier lassen sich allgemeine Regelungen zur Nutzung der privaten Geräte im Rahmen des BYOD-Modells abbilden, um eine Einheitlichkeit im Unternehmen herzustellen.

- **Nutzungsvereinbarung/Einwilligungserklärung**
  Da Betriebs- bzw. Personalrät:inn nicht über die privaten Geräte der Beschäftigten bestimmen können, müssen die Mitarbeiter:innen ihre Bereitschaft zur Teilnahme am BYOD-Modell individuell erklären, die Regelungen anerkennen und in die Datenverarbeitung einwilligen – wobei Art. 7 DSGVO und in Hinblick auf die Freiwilligkeit der Einwilligung § 26 Abs. 2 BDSG zu beachten sind. Hierfür ist es zielführend, zwischen Arbeitgebenden und Mitarbeiter:innen eine individuelle Nutzungsvereinbarung zu BYOD zu treffen, die vertragliche Regelungen zur Nutzung des privaten Endgeräts, Kostenerstattung durch Arbeitgebende und Mitteilungspflichten bei Verlust oder Diebstahl enthält. In diesem Zuge sollte auch auf die technische Dokumentation verwiesen werden.

Fazit

Die Einführung eines BYOD-Modells hat viele Vorteile. Die Beschäftigten können im Rahmen eines BYOD-Modells ihr eigenes, modernes Gerät, das sie kennen und schätzen, für die betriebliche Nutzung verwenden

Die Vorteile von BYOD

+ Mitarbeiter:innen müssen nur EIN Gerät mitführen
+ Erhöhung der Zufriedenheit der Beschäftigten z. B. durch Nutzung neuester Geräte
+ Steigerung der Produktivität und Erreichbarkeit
+ Sinkender Schulungsbedarf dank vertrauter Tools
+ Bessere Identifikation mit den Arbeitgebenden
+ Geringere Anschaffungskosten für die Arbeitgebenden

Gleichzeitig sind zahlreiche rechtliche Herausforderungen eines BYOD-Modells zu lösen.

Die Herausforderungen von BYOD

+ Verwaltung unterschiedlicher Mobilgeräte – eine Beschränkung auf bestimmte Hersteller ist anzuraten
+ Abdeckung der rechtlichen Aspekte durch Betriebsvereinbarung mit dem Betriebs- bzw. Personalrät:in und Nutzungsvereinbarungen sowie Einwilligungserklärungen mit den Mitarbeiter:innen
+ Ausräumung von Bedenken hinsichtlich Zugriffsmöglichkeiten der Arbeitgebenden auf private Daten, falls ein MDM zum Einsatz kommt

Auf Freiwilligkeit von BYOD achten

Die Teilnahme an einem BYOD-Modell muss für die Beschäftigten immer freiwillig möglich sein. Meist wird der Wunsch nach der Einführung eines BYOD-Modells aber vonseiten der Beschäftigten an die Unternehmens- bzw. Behördenleitung herangetragen. Kein(e) Mitarbeiter:in kann jedoch zur Teilnahme verpflichtet werden, da zwingend erforderliche Arbeitsmittel von den Arbeitgebenden zu stellen sind.[5]

BYOD, erlauben oder verbieten?

Durch die Verwendung einer entsprechenden Anwendungssoftware und durch den Abschluss entsprechender oben beschriebener Vereinbarungen lassen sich die Vorteile für Beschäftigte und Unternehmen optimal nutzen, rechtliche Herausforderungen lösen und Sicherheitsrisiken minimieren. Von dem Einsatz von privater Technik für berufliche Belange ohne ein BYOD-Modell und ohne die hier beschriebenen technischen und organisatorischen Regelungen sollte abgesehen werden, da sich hierdurch erhebliche Risiken ergeben.

Seit der Geltung der Datenschutzgrundverordnung (DSGVO) ab Mai 2018 hat sich dabei das Bußgeldrisiko erheblich erhöht, das bei einer Verletzung des Datenschutzrechts droht. Die DSGVO sieht Bußgelder von bis zu 20 Millionen Euro bzw. 4 Prozent des gesamten weltweiten Jahresumsatzes vor.

5 Vgl. LAG Hessen, Urteil vom 12.03.2021, Az. 14 Sa 306/20.

MATERNA Virtual Solution

Lösungsempfehlung: SecurePIM von Materna Virtual Solution

Höchste Sicherheit und intuitives, mobiles Arbeiten – SecurePIM erfüllt beides. Beschäftigte können auf ihrem eigenen Gerät von überall bequem, sicher und DSGVO-konform auf E-Mails, Kontakte, Kalender, Messenger, webbasierte Fachanwendungen und Dokumente zugreifen. Personenbezogene Daten sind dabei mobil genauso wirkungsvoll vor fremden Zugriffen geschützt wie Behördendaten und Geschäftsgeheimnisse. Die SecurePIM App ist plattformübergreifend auf iOS und Android einsetzbar und kann auch mit neuesten Geräten genutzt werden.

BYOD-ready: SecurePIM deckt rechtliche Herausforderungen ab:

+ Strikte Trennung der privaten von den beruflichen/dienstlichen Daten, auf die nur im abgeschotteten Bereich der App zugegriffen werden kann
+ Verschlüsselte Aufbewahrung der Daten auf dem Gerät
+ Verschlüsselte Versendung von E-Mails
+ Verschlüsselte Übertragung der Daten vom Server zum Gerät – ohne VPN
+ Möglichkeit der Fernlöschung für Arbeitgebende

SecurePIM – die Kommunikationslösung für technisch und rechtlich abgesicherte BYOD-Modelle

Wenn auch Sie **hochsicheres, DSGVO-konformes Arbeiten von überall** für Ihre Mitarbeiter:innen realisieren möchten, dann sprechen Sie mit uns über **SecurePIM**!

kontakt@virtual-solution.com
T +49 89 30 90 57-0

MATERNA
Virtual Solution

Über Materna Virtual Solution

Materna Virtual Solution, ein Unternehmen der Materna-Gruppe, ist ein auf sichere mobile Anwendungen spezialisierter Softwarehersteller mit Sitz in München und Entwicklungsstandort in Berlin.

Das Unternehmen entwickelt und vertreibt die Applikationen SecurePIM, SecureCOM und die Sicherheitsarchitektur SERA für iOS und Android. SecurePIM ermöglicht verschlüsseltes und benutzerfreundliches mobiles Arbeiten. Behörden können mit Smartphones und Tablets auf Geheimhaltungsstufe VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) und auf der Sicherheitsstufe NATO RESTRICTED kommunizieren.

Für Unternehmen stellt SecurePIM die Anforderungen der Datenschutzgrundverordnung (DSGVO) auf mobilen Geräten sicher und senkt damit die Risiken strafbewährter DSGVO-Verstöße und des Verlustes von Unternehmensdaten.

Materna Virtual Solution wurde 1996 gegründet und beschäftigt rund 100 Mitarbeiter:innen. Alle Produkte der Materna Virtual Solution tragen das Vertrauenszeichen »IT-Security made in Germany« des TeleTrust-IT-Bundesverbandes IT-Sicherheit e.V.

MATERNA
Virtual Solution

Notizen

P-22.0080_Whitepaper_BYOD Rechtlich_v4_05/22

MATERNA
Virtual Solution

Materna Virtual Solution GmbH
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com