MATERNA
Virtual Solution

+ Aktuelle Daten zu Bring-Your-Own-Device erhalten
+ Problemen vorbeugen, Lösungen finden
+ Die wichtigsten rechtlichen Aspekte kennen
+ Entscheider überzeugen
+ Technologie-Tipp inklusive

BYOD-Modelle einfach und sicher umsetzen

Materna Virtual Solution GmbH · Januar 2024

MATERNA
Virtual Solution

Bringen Sie Ihr eigenes Gerät zur Arbeit mit!

So oder so ähnlich könnte man »Bring Your Own Device« (BYOD) übersetzen. Doch hinter der Abkürzung steckt weit mehr: Sie bezeichnet die Nutzung von privaten Endgeräten für berufliche Zwecke. Dazu zählt nicht nur die private Hardware wie z. B. Smartphones und Tablets, sondern auch die private Software. In Deutschland arbeitet spätestens seit 2020 die Mehrheit der Beschäftigten mobil. 45 Prozent von ihnen, immerhin fast 20 Millionen Menschen, arbeiteten im Dezember des Pandemie-Jahres ganz oder teilweise von zu Hause[1]. Viele von ihnen nutzten dabei eigene Geräte – BYOD ist zur »Quick & Dirty«-Lösung vieler Organisationen geworden. Doch IT- und Datenschutzabteilungen stellte BYOD vor immense Herausforderungen bei der Sicherheit und Verwaltung. Und tut dies bis heute. Fragt sich: Wie können Unternehmen sowie Behörden Mitarbeitenden ermöglichen, überall produktiv zu sein, ohne dabei Datenverluste mit kostspieligen Folgen zu riskieren? Lesen Sie, wie Sie ein nachhaltiges und sicheres BYOD-Modell einführen!

Nach diesem Whitepaper kennen Sie

- aktuelle Studienergebnisse zu BYOD
- die Chancen von BYOD-Modellen für Unternehmen und Behörden
- und die größten Herausforderungen für die Verantwortlichen
- wesentliche rechtliche Aspekte, die zu beachten sind
- eine technische Lösung für sicheres Arbeiten mit Privatgeräten
- Argumente, die Entscheider:innen überzeugen

1 Zu dem Ergebnis kommt eine repräsentative Umfrage des Digitalverbands Bitkom: https://www.bitkom.org/Presse/Presseinformation/Mehr-als-10-Millionen-arbeiten-ausschliesslich-im-Homeoffice

MATERNA
Virtual Solution

Inhalt

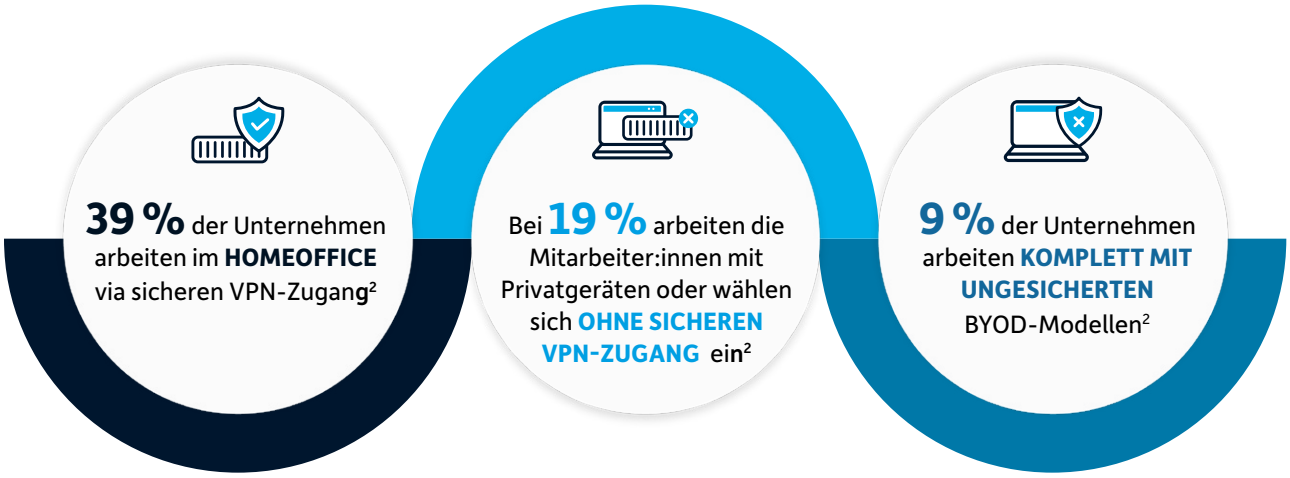
Seite

MATERNA Virtual Solution

BYOD: In der Regel ungeregelt

Blicken wir der Wahrheit ins Gesicht: Selten ist der berufliche Einsatz von Privatgeräten klar geregelt. Das liegt nicht allein an den Organisationen. Auch rechtlich wurde das Thema bisher eher stiefmütterlich behandelt, ist bisher ungeregelt und von daher eine rechtliche Grauzone. Doch die Pandemie und die darauf folgende »Disruption im Homeoffice« hat neue Tatsachen geschaffen. Die IT-Anschaffung wurde in unternehmerischer Not zeitweilig »outgesourct« und war den Mitarbeiter:innen überlassen. Dabei blieb gerade das Thema Datensicherheit auf der Strecke. Was eine Studie des TÜV Süd von 501 deutschen Unternehmen im Februar 2021 bestätigt:

Und die verbleibenden 33 Prozent? Sie verbieten BYOD pauschal und verhindern damit Engagement der Mitarbeitenden, das gerade in Krisenzeiten überlebenswichtig ist. Intelligente Organisationen haben erkannt, dass BYOD ein geeignetes Werkzeug ist, um jederzeit geschäftsfähig zu sein. Da wäre es doch das Beste, man löst die Herausforderungen, die sich bei BYOD-Modellen zwangsläufig ergeben. Gehen wir es also an und finden Lösungen!



2 https://blog.wiwo.de/look-at-it/2021/03/18/ein-jahr-corona-lockdown-zwei-von-fuenf-firmen-haben-home-office-zugaenge-abgesichert/

MATERNA
Virtual Solution

BYOD-Strategien und ihre Herausforderungen

1. Datensicherheit

Wie soll man sensible Daten auf einem Privatgerät schützen und Reputationseinbußen im Falle von Datenverlust oder -missbrauch vermeiden? Eine Frage, die Verantwortliche klären müssen.

2. Compliance

Datenschutzbeauftragte, die etwas auf sich halten, wissen: Die DSGVO gibt eine strikte Trennung von privaten und geschäftlichen Daten vor. Ist das auf einem Privatgerät technisch überhaupt möglich?

3. Kosten

Die Geräte gehören den Mitarbeitenden – damit fallen weniger Hardware-Investitionen an. Doch wer kommt für die anfallenden Kosten der Nutzung wie Datenverbrauch & Co. auf? Wie trennt man geschäftliche von privaten Kosten? Das interessiert nicht nur Ihre Finanz-Abteilung!

4. IT-Support

Bevor Ihre IT-Abteilung S.O.S. sendet: Wie soll man unterschiedlichste Privatgeräte verwalten, ohne immensen Aufwand bei den Administrator:innen zu verursachen?

5. Rechtliche Aspekte

Was passiert eigentlich, wenn das geschäftlich genutzte Privatgerät gestohlen wird? Wie lassen sich Urheberrechtsschutz und Aufbewahrungspflichten auch bei BYOD-Modellen wahren? Das will die Rechtsabteilung sicher ganz genau wissen. Wir geben einen Überblick über das nötige Vertragswerk.

6. Work-Life-Balance

Bei aller Flexibilität und Begeisterung für »New Work«-Modelle: Die Teilnahme an BYOD-Modellen muss für Mitarbeitende freiwillig bleiben und arbeitnehmerfreundlich sein. Da haben auch die Betriebs- und Personalrät:innen ein Auge drauf!

Vieles, was bedacht sein will! Wenn Ihnen dieser Überblick gerade die Schweißperlen auf die Stirn getrieben hat, dürfen wir sie gleich beruhigen. Es gibt rechtliche und technische Lösungen für all diese BYOD-Herausforderungen. Man muss sie nur kennen. Hier folgen Antworten auf diese Fragen:

1. BYOD & Datensicherheit: Sollte man nicht auf die leichte Schulter nehmen

Datenlecks und Cyberangriffe belasten Unternehmen aller Branchen und Größen sowie Behörden schwer. Besonders auch für Betreiber kritischer Infrastrukturen, wie Krankenhäuser oder Wasserversorger, steht bei Ausfällen weit mehr auf dem Spiel als der gute Ruf. Während viele ihre stationären Geräte in den Büros und Produktionsstätten mittlerweile solide absichern, lassen nicht wenige dies in Homeoffice und Außendienst schleifen. Damit stehen sie nicht allein. Selbst Digitalvisionäre wie Amazon-Gründer Jeff Bezos, die es eigentlich besser wissen müssten, sind nicht vor unerwünschten Zugriffen auf ihre beruflich eingesetzten mobilen Privatgeräte gefeit[3]. Aktuelle Studien bestätigen einen Anstieg der Vorfälle im Pandemie-Jahr 2020:

Alle 39 Sekunden findet ein Cyberangriff statt.[4]

Um 112.349 € stiegen die Kosten für Datenschutzverletzungen durch Remote Work in 2020[5]

95 % der Sicherheitsverstöße werden durch menschliches Fehlverhalten verursacht.[6]

Lösung: Tools einsetzen, die dem »Privacy by Design«-Ansatz folgen

Für Management- und IT-Sicherheitsverantwortliche hat der Schutz wertvoller Unternehmensdaten oberste Priorität. Sie bzw. die dahinterliegenden Informationen sind in den digitalen Geschäftsmodellen von heute eine »harte« Währung. Genauso wichtig sollte der Schutz von Mitarbeiter:innendaten sein. Arbeitgeber:innen sind übrigens durch die DSGVO verpflichtet, technische und organisatorische Maßnahmen (so genannte TOMs) zu treffen. Aufsichtsbehörden können bei Verstößen gegen Art. 32 der DSGVO, der die TOMs beschreibt, Bußgelder von bis zu 10 Millionen Euro oder von bis zu 2 Prozent des gesamten Jahresumsatzes verhängen. Also schon dann, wenn Unternehmen die TOMs nicht nachweisen können – auch ohne dass es hierdurch zu einem Datenschutzverstoß gekommen sein muss.

Aufsichtsbehörden können bei Verstößen Bußgelder von bis zu 20 Millionen Euro oder von bis zu 4 Prozent des gesamten Jahresumsatzes verhängen.
(Art. 83 Abs. 4 DSGVO)

3 https://www.wiwo.de/technologie/digitale-welt/cybersecurity-mein-tipp-an-bezos-dienstliches-und-privates-auf-dem-smartphone-trennen/25467556.html
4 https://blog.wiwo.de/look-at-it/2021/03/09/cybersicherheit-die-wichtigsten-zahlen-fakten-zu-datenschutz-verletzungen-2021/?fbclid=IwAR3Z_Cik5Nv__I0KzucxJR4zB3dKEQvx6GTGNLAnnLPBK4miGWPbj1b3pdo
5 www.varonis.com/blog/cybersecurity-statistics/
6 https://www.cybintsolutions.com/cyber-security-facts-stats/

MATERNA
Virtual Solution

Privacy by design: Lösungen, denen Sicherheit in den Code geschrieben ist

Empfehlung: Setzen Sie auf Datensicherheit out-of-the-box mit »privacy by design« bzw. »privacy by default« wie es die Aufsichtsbehörden voraussetzen. Das bedeutet: Nutzen Sie Lösungen, bei denen Datenschutzaspekte schon während der Entwicklung mit einbezogen wurden und nicht erst im Nachhinein.

> **Ein Tipp:** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) prüft und empfiehlt kontinuierlich technische Lösungen deutscher Hersteller, die mobiles Arbeiten auf Smartphones und Tablets sicher ermöglichen. Informieren Sie sich und agieren Sie entsprechend!

Deutsche Wohnen zahlt 2019 hohes Lehrgeld in Sachen Datenschutz

Was geschieht, wenn Unternehmen untätig bleiben, zeigt übrigens der Fall der »Deutsche Wohnen« 2019. Die Berliner Datenschutzbehörde verhängte ihr als einem der ersten deutschen Unternehmen ein Bußgeld – in der Höhe von 14,5 Millionen Euro: »Mit ihrer Millionenstrafe nimmt die Behörde einen strukturellen Mangel bei der Deutsche Wohnen aufs Korn. Das Archivsystem verstoße sowohl gegen die Grundsätze der Datenschutzgrundverordnung (Artikel 5 DSGVO) als auch gegen das Gebot des Datenschutzes durch Technikgestaltung (Artikel 25 DSGVO). Der Fall ist auch deshalb von besonderer Bedeutung, weil dieses »Privacy by Design« genannte Gebot mit der DSGVO neu eingeführt wurde und bisher kaum mit Leben gefüllt ist.«[7]

Lektüre-Tipp: So gestalten Sie Ihre Technik DSGVO-konform

Mehr Informationen zu »privacy by design« bzw. »privacy by default« und deren Vorteile erfahren Sie in unserem → *Blog-Beitrag*.

7 https://netzpolitik.org/2019/datenschutzgrundverordnung-deutsche-wohnen-erste-millionenstrafe/

MATERNA
Virtual Solution

2. BYOD & Compliance: Undankbare Aufgabe für Datenschutzbeauftragt:innen?

Viele Unternehmen stehen BYOD-Programmen für den Einsatz privater Smartphones oder Tablets grundsätzlich positiv gegenüber. Zurecht, denn BYOD bringt viele Vorteile: So kann beispielsweise die Produktivität der Mitarbeiter:innen und ihre Zufriedenheit erheblich steigen. Mobile Geräte und Apps sind meist komfortabler und benutzerfreundlicher als stationäre Rechner oder Unternehmenssoftware. Gerade jüngere und Mitarbeitende z. B. im Außendienst wollen und müssen von unterwegs schnell und flexibel mit den ihnen bekannten Tools arbeiten können, am liebsten natürlich von ihrem privaten Gerät. Doch Unternehmen sind auch an geltendes Recht und Vorgaben der Aufsichtsbehörden gebunden. Oft entsteht hier ein Zielkonflikt zwischen Compliance und Unternehmens- bzw. Anwender:innenbedürfnissen – also aus Datenschutz und ihrer Nutzung.

Lösung: Daten trennen mit der Container-Technologie

Die häufig undankbare Aufgabe, Compliance-Vorgaben zu erfüllen, kommt dem Datenschutzbeauftragte:innen zu. Wo liegt das Problem? Über die Sicherheitsanforderungen der Unternehmens-, Behörden-, Kunden- und Bürgerdaten hatten Sie sich auf den Vorseiten bereits informiert. Doch was ist mit den persönlichen Daten der Mitarbeiter:innen? Die Kombination aus privatem Endgerät und Kontrolle durch die Arbeitgebenden kann zu rechtlichen Problemen führen. BYOD-Geräte enthalten private Daten der Mitarbeitenden wie Familienfotos oder Informationen aus sozialen Netzwerken. Es besteht also die reale Gefahr, dass diese bei Cyberattacken ebenfalls in die falschen Hände geraten.

Big Brother is watching? Via Mobile-Device- Management zumindest nicht unmöglich

Ein weiteres Problem, das zunehmend auch Betriebsrät:innen umtreibt: Theoretisch könnten IT-Administrator:innen über Mobile-Device-Management (MDM), mit denen die Endgeräte gesteuert werden, auf private Daten der Mitarbeiter:innen zugreifen. Schlimmer noch, die Gänge und Wege der Mitarbeiter:innen ließen sich tracken. Ein echtes Big-Brother-Szenario, bei dem für Datenschutzverantwortliche die Alarmglocken schrillen. Das zweite Problem lässt sich mit BYOD-tauglichen Lösungen beheben, die ganz auf ein MDM verzichten. Mehr dazu in unserem Technologie-Tipp.

Für das erste Problem empfiehlt die DSGVO selbst ein praktikables und sicheres Lösungskonzept: Die Trennung von privaten und beruflichen Daten auf ein und demselben Gerät. Klingt gut, nur wie setzt man das technisch um?

Trennt konsequent privat und beruflich: Die Container-Technologie

Die Trennung von Privatem und Beruflichem ist technologisch längst machbar – wenn man auf die richtige Lösung setzt. Hier hat sich die sogenannte Container-Technologie bewährt. Kommunikationslösungen, die darauf basieren, legen den Fokus auf den Schutz der Daten auf mobilen Endgeräten und sind unabhängig von der Sicherheit des darunterliegenden Betriebssystems. Entsprechende Lösungen schotten Unternehmens-, Behörden- und Anwender:innendaten, E-Mails, Telefonie, Messenger-Funktionen und Dokumente in einem verschlüsselten Bereich ab. Damit lassen sich berufliche Daten auf dem mobilen Gerät in einer geschützten Umgebung bearbeiten und verwalten. Informationen sind vor unautorisierten Zugriffen, Verlust oder Manipulation geschützt und können nicht unkontrolliert ab- oder einfließen.

Privatsphäre der Mitarbeitenden schützen, Unternehmensdaten sichern

Container-Lösungen gewährleisten somit die strikte Trennung von beruflichen und privaten Daten, die der Datenschutz vorsieht. Das heißt: Nutzer:innen können aus dem abgeschotteten Bereich heraus nicht auf ihre privaten Apps zugreifen. So verhindert die Technologie beispielsweise, dass interne Informationen per Copy & Paste auf Facebook oder Twitter landen oder datenhungrige Messenger-Apps auf Geschäftskontakte zugreifen. Zugleich schützt die Container-Technologie die Privatsphäre der Mitarbeiter:innen. Das nimmt ihnen die Angst, von der eigenen IT-Abteilung »ausspioniert« zu werden. Denn auch hier gilt: Privates bleibt privat. Die IT kann, z. B. bei Verlust oder Diebstahl lediglich auf die beruflichen Daten im Container des privaten Smartphones oder Tablets zugreifen.

> **Gut zu wissen:** Die Datenübertragung wird bei Container-Technologien über ein Gateway verschlüsselt. Es sichert so die Informationen während der Übermittlung – ganz ohne umständliche VPN-Infrastruktur.

MATERNA
Virtual Solution

3. BYOD & Kosten: Bei der Hardware sparen, die Nutzung regeln

BYOD-Modelle haben unter Ihren zahlreichen Vorteilen auch den des Kostenaspekts. Eine Digitalisierungsstrategie, die nicht auf der Neuanschaffung von mobilen Dienstgeräten basiert, sondern ganz oder teilweise auf dem Einsatz der Privatgeräte von Mitarbeiter:innen ist budgetschonend. Doch »gratis« sind natürlich auch BYOD-Modelle nicht zu haben. Arbeitnehmer:innen haben bei Teilnahme an diesen Modellen auch Rechte auf Kostenübernahmen bei Mobilfunkverträgen und Co. Diese zunächst versteckten Kosten lassen sich nach Rücksprache gut beziffern und mit Nutzungsvereinbarungen regeln.

Lösung: Durchdachte Kostenstrategie entwickeln

VOR der Einführung eines BYOD-Modells macht es Sinn, sich zu überlegen, wie man das Thema im Unternehmen strategisch am besten angeht. Ein Finanzplan und schriftliche Vereinbarungen, die genau diese Themen nachvollziehbar regeln, sind empfehlenswert. Controlling und Steuerberatung sollten zudem prüfen, ob durch Kostenübernahmen geldwerte Vorteile entstehen, die dann zu versteuern wären. Auch das müssen Mitarbeiter:innen wissen.

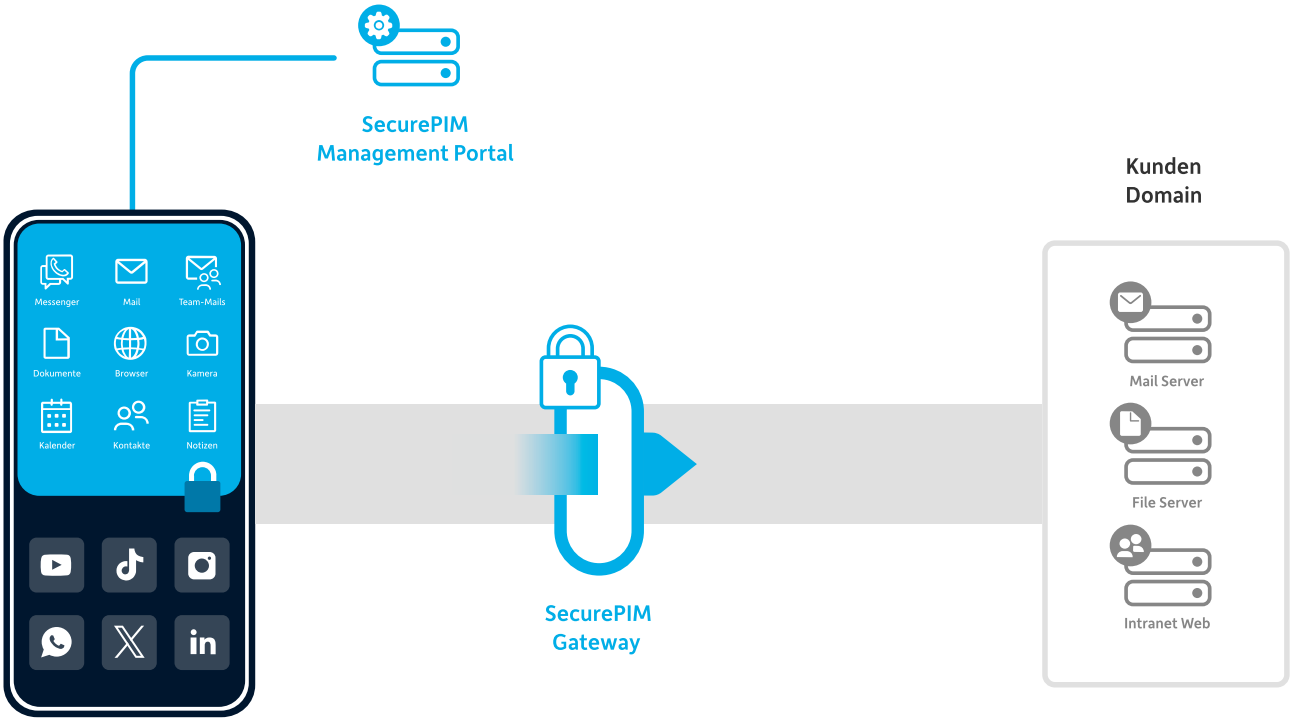
MATERNA
Virtual Solution

4. BYOD & IT-Support: »Bring Your Own Desaster«

So praktisch BYOD für Anwender:innen ist, für IT-Administrator:innen erhöhen sich Aufwände dadurch oft. Einerseits widerspricht die Vielzahl der privaten Endgeräte ihrem Bedürfnis nach Standardisierung. Schließlich muss die IT alle gängigen mobilen Betriebssysteme unterstützen, zum Beispiel Apple iOS und Google Android. Mit der privaten Nutzung verschwimmen zudem die Grenzen zwischen privaten und Unternehmensdaten. Zudem bringen Nutzer:innen immer ihr eigenes privates »IT-Chaos« mit. Die Befürchtungen, die Kontrolle über die unternehmenseigenen Daten zu verlieren, sind also berechtigt. Weitere Probleme können die Geräteverwaltung, Berechtigungen und Sicherheitsprodukte machen, ganz zu schweigen vom Support am Service Desk. Doch eine IT-Abteilung, die BYOD verbietet, schafft automatisch eine Schatten-IT. Das kann also nicht die Antwort sein.

Lösung: Geräteunabhängige Alleskönner einsetzen

Für ein Aufatmen in der IT-Abteilung können All-in-one-Lösungen sorgen, die nicht nur mit Verschlüsselung und Container-Technologie für Datensicherheit sorgen, sondern auch Konfiguration und Roll-out im Self-Service bieten: Mitarbeiter:innen können sich die Anwendung aus dem App Store oder bei Google Play selbst herunterladen und sofort nutzen. Die Installation eines Mobile-Device-Management-Profils ist nicht nötig. Zusätzliche Entlastung bieten integrierte Management-Portale, die es Administrator:innen erlauben, Sicherheitsregeln festzulegen, Passwortlängen und Funktionen anzupassen. So behalten sie die Kontrolle über die geschäftliche IT. Wichtig hierbei: Auf Geräteunabhängigkeit achten, also mit einer Lösung arbeiten, die für alle Betriebssysteme und alle mobilen Geräte im Unternehmen funktioniert. Eine dieser Lösungen ist SecurePIM. Details dazu später in diesem Whitepaper.



5. BYOD & Rechtliche Aspekte: Regelungen jenseits der DSGVO

Selten geregelt, oft bedauert: BYOD-Modelle sind in vielerlei Hinsicht abzusichern. Auch jenseits von Datenschutzverordnungen wie der DSGVO. Tun Sie sich selbst den Gefallen und machen Sie den BYOD-Einsatz in Ihrem Unternehmen »wasserdicht« – mit dem entsprechenden Vertragswerk, gestaltet von juristischen Profis. Das spart Ihnen und allen Betroffenen Kummer, Aufwand und letztendlich auch viel Geld.

Lösung: Umfangreiches Vertragswerk aufsetzen lassen

Wir haben Ihnen hier eine kurze Checkliste über die im Unternehmen einzubeziehenden Stellen und das teilweise recht umfangreiche Vertragswerk zusammengestellt.

Quick-Check 1: Relevante Abteilungen

Wenn Sie ein BYOD-Modell einführen, betrifft das viele Mitarbeitende. Hier folgt eine Kurzübersicht über die relevanten Abteilungen, 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 Vielfältigkeit der privaten Geräte ergibt sich für die IT ggf. ein höherer administrativer Aufwand.

+ **Personalabteilung**
  HR ist zuständig für zu unterzeichnende Mitarbeiter:innenvereinbarungen 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 Mitarbeiter:innnenvereinbarung erstellen und ggf. mit dem Betriebs- bzw. Personalrat verhandeln.

+ **Datenschutzbeauftragt:innen**
  Sie sind bei der Verarbeitung personenbezogener Daten immer hinzuzuziehen. Kenntnisnahme der BYOD-Einführung und eine korrekte Abwicklung des Vertragswerks dazu sind also sinnvoll.

Quick-Check 2: Wesentliche Dokumente

Nachdem Sie die betreffenden Abteilungen informiert haben, benötigen Sie das passende Vertragswerk für eine rechtssichere Einführung. Hier eine Übersicht über die relevanten Dokumente:

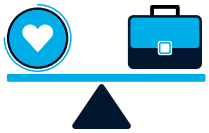
+ **Technische Dokumentation mit Freigabeformular**
  Hier sollte geregelt sein, mit welchem Gerät Beschäftigte jeweils am BYOD-Modell teilnehmen möchten, wie die Installation abläuft und wer die Teilnahme genehmigt hat.

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

+ **Nutzungsvereinbarung/Einwilligungserklärung**
  Da Betriebs- bzw. Personalrät:innen nicht über die privaten Geräte der Beschäftigten bestimmen können, müssen die Mitarbeiter:innen ihre Bereitschaft zur Teilnahme am BYOD-Modell individuell ausdrücken, die Richtlinien anerkennen und in die Datenverarbeitung einwilligen.

Lektüre-Tipp: BYOD-Modelle rechtssicher aufstellen

Mehr zu den rechtlichen Aspekten von BYOD finden Sie in unserem Whitepaper → *»BYOD-Modelle rechtlich absichern«*, das in Zusammenarbeit mit der Rechtsanwaltskanzlei Heussen entstanden ist.



6. BYOD & Work-Life-Balance: Was Mitarbeitende wollen & Personalgremien fordern

Es gibt unzählige BYOD-Vorteile für Mitarbeiter:innen, von denen unmittelbar auch das ganze Unternehmen profitiert. Hier sind fünf gewichtige:

+ Mitarbeiter:innen müssen nur ein Gerät mitführen
+ ihre Produktivität und Erreichbarkeit steigern sich
+ der Schulungsbedarf sinkt dank vertrauter Geräteoberflächen
+ die Zufriedenheit der Beschäftigten wächst
+ die Identifikation mit den Arbeitgeber:innen wird besser

Von der Flexibilität, die das New-Work-Modell auf Basis von Privatgeräten mit sich bringt, profitiert der vertriebliche Außendienst in Finanzinstituten genauso wie die Service-Techniker:innen in öffentlichen Unternehmen, Ärzt:innen am Patientenbett, mobile Pfleger:innen, Anwält:innen, aber auch freie bzw. temporäre Mitarbeiter:innen in Forschungsinstituten.

Die Erlaubnis, private Endgeräte bei der Arbeit nutzen zu dürfen, kann Unternehmen und Behörden auch vor dem Hintergrund der »Work-Life-Balance« als Arbeitgeber:in attraktiver machen. In Zeiten des drohenden Fachkräftemangels ist das ein nicht zu unterschätzender Faktor. Doch natürlich hat alles auch seine Nachteile:

Sicher möchten Ihre Mitarbeiter:innen und der Personalrat z. B. wissen, wie der Feierabend auch bei theoretisch ständiger Erreichbarkeit garantiert bleibt. Wie man Mitarbeiter:innen ggf. vor sich selbst schützt und Wochenend- bzw. Arbeit nach Betriebsschluss unterbindet.

BYOD Vorteile

Für die Teilnehmer des Zukunftspanel »Staat und Verwaltung« 2021 liegen die Vorteile auf der Hand:[8]

Lösung: Kooperation mit und Schutz von Mitarbeiter:innen

Hier gilt es, rechtzeitig eine gute und nachvollziehbare BYOD-Strategie zu durchdenken und gezielt mit den Mitarbeiter:innen dazu zu kommunizieren. Suchen Sie vor der Einführung von BYOD-Modellen den Kontakt zu Ihren Mitarbeiter:innen und deren Vertretungen in Personal- bzw. Betriebsratsgremien. Denn eins liegt auf der Hand: Wer sich als Mitarbeiter:in gehört, gesehen und geschätzt fühlt, ist bereit, zu unterstützen und freiwillig produktiv zu sein. Um ganz Eifrige im Zweifel vor sich selbst zu schützen, sorgen technische Lösungen, wie z. B. SecurePIM dafür, dass Arbeitszeiten eingehalten werden. Sei es mit dem automatischen Ausloggen aus der App nach Dienstschluss oder dem Ausschalten von E-Mail-Benachrichtigungen nach Feierabend.

8 https://www.virtual-solution.com/infografik-zukunftspanel2021-byod/

MATERNA Virtual Solution

Fazit BYOD: Erlauben, statt verbieten

Am einfachsten und sichersten geht das mit einer Kommunikationslösung, die sich im Markt bewährt hat und vom BSI zugelassen und empfohlen ist: mit SecurePIM von Materna Virtual Solution.

SecurePIM – die Kommunikationslösung für technisch und rechtlich abgesichertes BYOD

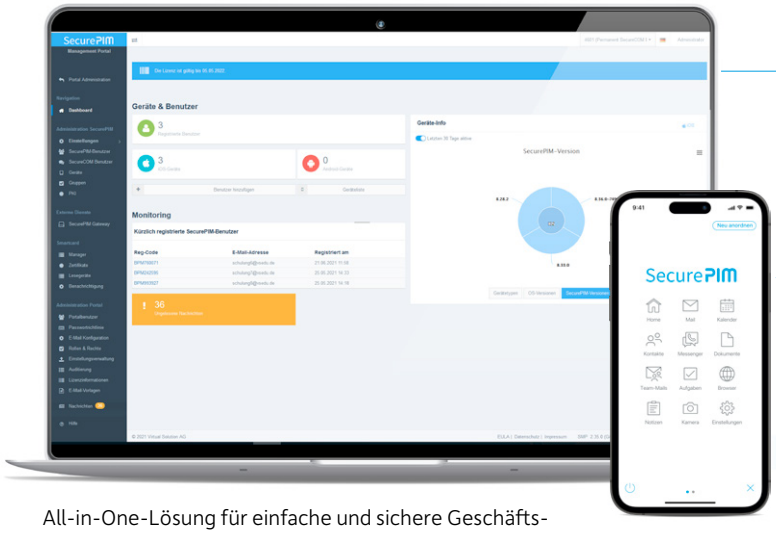
Mit der Kommunikationslösung SecurePIM kommt alles, was Sie und Ihre Mitarbeiter:innen für die Kommunikation über mobile Endgeräte benötigen, sicher und einfach in einer App. SecurePIM schottet E-Mails, Intranet-Zugang und mehr auf mobilen iOS- sowie Android-Geräten in einem verschlüsselten Containerbereich ab. Die Daten sind via Passwort, PIN oder Identifikation per Fingerabdruck und Gesichtserkennung zugänglich.

Mobiles Arbeiten auf dem eigenen Gerät – BYOD mit der SecurePIM App:

+ E-Mails mit Verschlüsselung
+ Kalender mit Zugriff auf freigegebene Kalender
+ Kontakte mit Anzeige der Anrufer:innen
+ Kamera mit verschlüsselter Ablage im Container
+ Dokumente mit Editierfunktion und Fileshare-Zugriff
+ Browser mit Zugriff auf Intranet und Web-Apps
+ Integrierter Messenger mit verschlüsseltem Chat
+ Verschlüsselte Audio- und Videotelefonie

MATERNA
Virtual Solution

Aus diesen Komponenten besteht SecurePIM von Materna Virtual Solution:



All-in-One-Lösung für einfache und sichere Geschäftskommunikation auf privaten Endgeräten.

1. **SecurePIM Management Portal**
   für Konfiguration, Verteilung und Kontrolle als Cloud und On-Premises Lösung
2. **SecurePIM App**
   für sicheres mobiles Arbeiten mit iOS & Android
3. **SecurePIM Gateway**
   Für sicheren Zugriff auf die Unternehmens-Infrastruktur

Einmal SecurePIM und gleich vier Sorgen weniger

1. **Strafzahlungen und Reputationsverlust vermeiden:** SecurePIM ist out-of-the-box DSGVO-konform. Auch auf privaten Mobilgeräten.
2. **Hardware-Kosten sparen, Zufriedenheit der Mitarbeiter:innen steigern:** SecurePIM ermöglicht BYOD- und COPE-Modelle gleichermaßen
3. **Umfassender Geheimnisschutz bis zu** VS-NfD: Mobiles Arbeiten mit besonders schützenswerten Daten und Zertifizierungen für z. B. TISAX®, Geheimnisschutzgesetz etc.
4. **Maximaler Anwenderkomfort dank intuitiver Bedienung:** SecurePIM sorgt für einen schnellen Start und wenig Schulungs- und Verwaltungsaufwand bei Mitarbeitenden sowie Administrator:innen.

MATERNA
Virtual Solution

Mit SecurePIM setzen Sie den Fokus auf Ihre Daten statt auf Geräte

Ein Mobile-Device-Management, wie Sie bzw. wahrscheinlich eher Ihre IT-Expert:innen es bisher kannten, kann mit SecurePIM in den meisten Fällen entfallen. Denn statt bisher den Fokus des Schutzes auf die einzelnen Mobilgeräte im Unternehmen zu legen, rücken Sie mit SecurePIM den Schutz Ihrer sensiblen Unternehmensdaten in den Vordergrund. Der Unterschied und die Vorteile liegen auf der Hand:

Vorteile SecurePIM

+ Mitarbeiter:innen müssen nur eine App installieren, um mobil arbeiten zu können
+ weitere Modifikationen am Privatgerät sind nicht notwendig
+ geringer Aufwand für die IT, da nur die SecurePIM App zu verwalten ist
+ einheitliche Strategie für iOS & Android
+ ist bereits ein MDM-Tool im Einsatz unterstützt SecurePIM auch dieses Szenario

Wann ist dennoch ein MDM-System notwendig?

+ wenn Ihre IT selbstentwickelte Apps verteilen muss
+ wenn die App-Installation auf Mobilgeräten kontrolliert werden soll
+ wenn Mobilgeräte über GPS ortbar sein sollen

> **Gut zu wissen:** SecurePIM ist nicht nur bei BYOD die richtige Wahl, sondern auch für Company-Owned-Personally-Enabled, so genannte COPE-Modelle. Also für die Nutzung von Unternehmens-IT für private Zwecke. Damit kann zum Beispiel die Überlassung eines betrieblichen Smartphones für Privatgespräche gemeint sein.

MATERNA
Virtual Solution

Sie möchten ein rechtlich und technisch sicheres BYOD-Modell in Ihrem Unternehmen oder Ihrer Behörde einführen? Sprechen Sie mit uns!

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

Über Materna Virtual Solution

Materna Virtual Solution, ein Unternehmen der Materna-Gruppe, ist ein marktführender Softwarehersteller mit Mobile Security Expertise ansässig in München und in Berlin, der sich auf Produkte und Beratungsleistungen im Bereich des sicheren ultramobilen Arbeitens spezialisiert hat.

Materna Virtual Solution konzentriert sich nicht nur auf die kontinuierliche Weiterentwicklung ihrer Applikation SecurePIM, sondern entwickelt auch Anwendungen für neue behördenspezifische Lösungen. SecurePIM basiert auf der Container-Technologie und versetzt Behörden in die Lage, mobil auf der Geheimhaltungsstufe Verschlusssachen – Nur für den Dienstgebrauch (VS-NfD) sowie auf der Sicherheitsstufe NATO RESTRICTED zu kommunizieren. Darüber hinaus entstehen im eigenen indigo Kompetenz-Center nicht nur neue Applikationen für das sichere ultramobile Arbeiten auf iPhones und iPads, auch die Umsetzung von kundenspezifischen Projekten sowie die Mobilisierung von Fachverfahren und Prozessen auf VS-NfD-Niveau sind Teil des umfangreichen Portfolios. Mit der Vision eines ultramobilen und sicheren Arbeitsplatzes bietet Materna Virtual Solution mit seiner umfassenden Expertise Beratungsleistungen entlang der gesamten Wertschöpfungskette an – unabhängig von den eingesetzten mobilen Plattformen und Betriebssystemen.

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

Materna Virtual Solution GmbH
Mühldorfstraße 8 · 81671 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com

P-23.0128_Whitepaper_BYOD Strategisch_de/de_v7_01/24