Virtual Solution

BRING YOUR OWN DEVICE

RECHTLICHE ASPEKTE

Bring your own device (BYOD) bedeutet, dass private Endgeräte (z.B. Smartphones) für berufliche Zwecke eingesetzt werden. Dies hat für den Arbeitnehmer und den Arbeitgeber Vorteile, es ergeben sich aber automatisch auch einige rechtliche Aspekte, die es zu beachten gilt.

Diese Kurzdarstellung gibt einen kurzen Überblick über die rechtlichen Aspekte, die bei der Einführung eines BYOD-Modells im Unternehmen zu beachten sind.

BYOD
RECHTLICHE ASPEKTE

BEI DER EINFÜHRUNG EINES BYOD-MODELLS ZU BEACHTENDE RECHTLICHE ASPEKTE

Datenschutz (unter BDSG und DSGVO)

Bei der Arbeit mit E-Mails und Dokumenten verarbeiten die Beschäftigten für den Arbeitgeber immer auch sog. personenbezogene Daten, also *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“*, die durch das Bundesdatenschutzgesetz (BDSG) geschützt sind, bzw. nach der Definition der Datenschutzgrundverordnung (DSGVO), die ab dem 25. Mai 2018 gelten wird, *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ((…) „betroffene Person“) beziehen; als identifizierbar wird 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“*.

Der Arbeitgeber ist die sog. *„verantwortliche Stelle“* im Sinne von § 3 Abs. 7 BDSG bzw. *„Verantwortlicher“* im Sinne von Art. 4 Nr. 7 DSGVO, d.h. er ist für die Einhaltung des Datenschutzes in Bezug auf die personenbezogenen Daten, die im Unternehmen verarbeitet werden (z.B. Kundendaten, Mitarbeiterdaten, usw.) verantwortlich. Er bleibt auch dann die verantwortliche Stelle, wenn seine Beschäftigten die Daten im Zuge eines BYOD-Modells auf ihren privaten Geräten verarbeiten.

Der Arbeitgeber ist und bleibt somit dafür verantwortlich, dass ausreichende technische und organisatorische Maßnahmen (sog. TOMs, vgl. § 9 BDSG bzw. Art. 32 DSGVO) getroffen werden, um die für die Einhaltung des Datenschutzes erforderlichen Anforderungen zu gewährleisten. Hierbei sind die getroffenen Maßnahmen schon unter dem BDSG in ein angemessenes Verhältnis zum angestrebten Schutzzweck zu setzten; unter der DSGVO müssen die vom Verantwortlichen und dem Auftragsverarbeiter getroffenen TOMs sogar explizit *„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. Dies bedeutet, dass der Arbeitgeber insbesondere Sorge dafür tragen muss, dass die personenbezogenen Daten auf dem Gerät des Beschäftigten so sicher sind, wie sie es auch auf der unternehmenseigenen IT-Infrastruktur des Unternehmens wären.

Die Sicherheit der Daten kann u.a. durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren gewährleistet werden (dies ist in der Anlage zu § 9 BDSG und in Art. 32 Abs. 1 lit. a) DSGVO auch so vorgesehen).

Bei einem BYOD-Modell gehen auch die datenschutzrechtlichen Aufsichtsbehörden[1] davon aus, dass die Daten des Unternehmens verschlüsselt gespeichert werden müssen und dass die beruflichen und die privaten Daten strikt zu trennen sind. Außerdem muss der Arbeitgeber die Möglichkeit haben, seine Daten – auch aus der Ferne – zu löschen.

Die Datenschutzgrundverordnung sieht auch vor, dass der Datenschutz bereits bei der Entwicklung neuer Produkte einbezogen und dass grundsätzlich mit datenschutzfreundlichen Voreinstellungen gearbeitet werden muss (*„privacy by design“* und *„privacy by default“*, Art. 25 Abs. 1 und 2 DSGVO). Beides Anforderungen, die auch beim BYOD eine wichtige Rolle spielen.

Mit der Datenschutzgrundverordnung ergibt sich hinsichtlich der technischen und organisatorischen Maßnahmen (TOMs) außerdem noch ein großer Unterschied zum BDSG: Bislang konnten die Aufsichtsbehörden ein Bußgeld nach dem BDSG nur durchsetzen, wenn es aufgrund mangelnder TOMs zu ei-

[1] Vgl. „Handreichung zur Nutzung von Smartphones und Tablet-Computer in Behörden und Unternehmen“ des Hessischen Datenschutzbeauftragten; Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), TB 2011/2012, S. 91.

BYOD
RECHTLICHE ASPEKTE

nem Datenschutzverstoß kam. Gemäß Art. 83 Abs. 4 DSGVO können die Aufsichtsbehörden u.a. bei Verstößen gegen Art. 32 DSGVO (der die TOMs beschreibt) Bußgelder von bis zu 10 Millionen Euro (oder von bis zu 2% des gesamten Jahresumsatzes) verhängen, also schon dann, wenn die TOMs „nur“ nicht nachgewiesen werden können (auch ohne dass es hierdurch zu einem Datenschutzverstoß gekommen sein muss). Es wird unter der DSGVO also schon negative Auswirkungen haben, wenn TOMs „nur“ nicht ausreichend dokumentiert worden sind, wenn eine Aufsichtsbehörde ein Bußgeld verhängen möchte. Außerdem werden sich die Bußgelder unter der DSGVO im Vergleich zu denen, die unter dem BDSG drohen (bis zu 50.000 EUR bzw. bis zu 300.000 EUR, gemäß § 43 BDSG), erheblich erhöhen!

Sind demgegenüber wirksame und geeignete TOMs umgesetzt und dokumentiert, die eventuell sogar über das „Übliche“ hinausgehen, kann dies bei der Bemessung der Höhe eines Bußgeldes nach der DSGVO positiv zu Gunsten des Verantwortlichen gewertet werden (vgl. Art. 83 Abs. 2 lit. d) DSGVO).

Geheimnisschutz

Mobile Endgeräte sind einer Vielzahl von potentiellen Bedrohungen ausgesetzt[2]. Bereits aufgrund der Größe und der Mobilität ist das Risiko des „Verlierens“ des Gerätes bzw. des Diebstahls erhöht. Die Möglichkeit der Fernlöschung dient daher u.a. auch dazu, sicherzustellen, dass Geschäfts- und Betriebsgeheimnisse des Unternehmens im Sinne von § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) nicht in die Hände von Unbefugten gelangen können. Geht das Gerät verloren oder wird es gestohlen, so können die Daten in einem verschlüsselten Container, der durch eine spezielle Anwendungssoftware erstellt wird, sicher gelöscht werden, so dass auch eine Entschlüsselung des Containers (soweit sie technisch überhaupt möglich sein sollte) nicht zu einem Abfluss von Unternehmensdaten führen würde.

Eine empfohlene zusätzliche Sicherheit wird durch die Möglichkeit der Ende-zu-Ende-Verschlüsselung von E-Mails geschaffen, so dass ein „Mitlesen“ durch Dritte ausgeschlossen bzw. erheblich erschwert wird.

Urheberrechtsschutz

Gemäß § 99 Urheberrechtsgesetz (UrhG) ist der Inhaber des Unternehmens (verschuldensunabhängig!) verantwortlich, wenn ein Arbeitnehmer ein Urheberrecht verletzt. Ein Urheberrecht könnte z.B. dadurch verletzt werden, dass ein Arbeitnehmer im Rahmen des BYOD-Modells eine Software beruflich einsetzt, die er privat erworben hat und die nur für die private Nutzung lizenziert ist (z.B. weil er die Nutzung dieser Software für „intuitiver“ hält als die Unternehmenssoftware). Trotzdem wäre der Unternehmensinhaber oder – wenn nicht sichergestellt ist, dass ernsthafte und geeignete Schutzvorkehrungen getroffen worden sind, um Urheberrechtsverletzungen zu verhindern – auch das Organ im Rahmen der Organhaftung (§ 43 GmbHG bzw. §§ 91 Abs. 2, 93 AktG) (persönlich!) hierfür haftbar.

Aufbewahrungspflichten

Die gesetzliche 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) müssen eingehalten werden. Sämtliche berufliche Kommunikation muss über den beruflichen E-Mail-Account geführt werden; es muss verhindert werden, dass geschäftsrelevante Kommunikation am Arbeitgeber „vorbeiläuft“.

[2]Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI),„Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“.

BYOD
RECHTLICHE ASPEKTE

Fazit

Die vorgenannten rechtlichen Anforderungen (v.a. Datentrennung, Verschlüsselung, Fernlöschung, Unterbinden von Copy-and-Paste) kann eine spezielle Anwendungssoftware (App) erfüllen.

Es wird hier ein verschlüsselter Container auf dem Gerät erstellt, der die privaten von den beruflichen Daten trennt. Zum Öffnen dieses Containers muss der Nutzer ein (zusätzliches und vom Gerätepasswort unabhängiges) Passwort eingeben, so dass Dritte keinen Zugriff auf die beruflichen Daten nehmen können.

DURCH ZUSÄTZLICHE VEREINBARUNGEN ABZUDECKENDE ASPEKTE

Im Rahmen eines BYOD-Modells müssen aber darüber hinaus einige weitere Punkte geregelt werden, die nur durch zusätzliche Vereinbarungen mit dem Beschäftigten und/oder dem Betriebs-/Personalrat abgedeckt werden können. Dies ist umso wichtiger, weil es zum BYOD weder spezifische Regelungen in Gesetzen gibt, noch – soweit bislang ersichtlich – Rechtsprechung zu dem Thema ergangen ist.

Sicherheit der Daten

Hierbei sind u.a. Vereinbarungen zu nennen, die für die Sicherheit der Daten wichtig sind: Der Beschäftigte verpflichtet sich immer ein aktuelles Betriebssystem sowie einen aktuellen Virenschutz einzusetzen, sein Gerät nicht zu „jailbreaken“ bzw. zu „rooten“ (d.h. die Nutzungsbeschränkungen des Herstellers nicht zu umgehen), sein Gerät nicht an Dritte weiterzugeben, seine privaten Daten selbst zu sichern, usw. Darüber hinaus ist zu regeln, in welchen Fällen eine (kurzzeitige) Herausgabe des Gerätes vom Beschäftigten verlangt werden darf. Für die Sicherheit der Daten müssen außerdem Regelungen zur Beendigung der Teilnahme am BYOD-Modell (auch durch Beendigung des Arbeitsverhältnisses) getroffen werden.

Mitteilungspflichten (unter BDSG und DSGVO)

Darüber hinaus müssen dem Beschäftigten Mitteilungspflichten auferlegt werden, z.B. bei Verlust/Diebstahl des Gerätes, damit zeitnah eine Fernlöschung durchgeführt werden kann. Außerdem muss sichergestellt sein, dass etwaige Informationspflichten des Unternehmens nach § 42a BDSG erfüllt werden können, wenn die dort genannten Daten unrechtmäßig übermittelt worden sein sollten oder einem Dritten unrechtmäßig zur Kenntnis gelangt sein könnten. Dies wird unter der Datenschutzgrundverordnung noch wichtiger, da die Meldepflicht dann zum einen nicht nur bei Datenpannen hinsichtlich „sensibler“ Daten gilt, sondern bei jeglicher Verletzung personenbezogener Daten (also z.B. auch bei einem bloßen Datenverlust, ohne dass es einer unrechtmäßigen Kenntnisnahme durch einen Dritten bedarf) erfolgen muss, und zum anderen, weil die Meldepflicht dann den Regelfall darstellt und nur dann nicht gemeldet werden muss, wenn *„die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“*. Darüber hinaus muss die Meldung nach Art. 33 DSGVO unverzüglich, möglichst innerhalb von 72 Stunden gemacht werden.

Neben der Meldepflicht gegenüber der Aufsichtsbehörde besteht – wie schon in § 42a Satz 2, 3, 5 BDSG – auch unter der Datenschutzgrundverordnung die Pflicht, die von der Datenpanne Betroffenen zu benachrichtigen. 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). Dies bedeutet, dass durch spezielle Anwendungssoftware, die personenbezogene Daten verschlüsselt, wie z.B. SecurePIM, die hohen Kosten, die durch solch eine Benachrichtigung der Betroffenen entstehen, und der daraus resultierende Imageschaden vermieden werden kann.

BYOD
RECHTLICHE ASPEKTE

Weitere Regelungsbereiche

Nachdem der Beschäftigte das Endgerät, das im Rahmen des BYOD-Modells beruflich genutzt werden soll, von einem Händler erworben hat oder es ihm vom seinem Mobilfunkanbieter während der Vertragslaufzeit zur Verfügung gestellt wird und nachdem das Eigentum weiterhin beim Beschäftigten verbleiben soll, stellen sich u.a. noch folgende Fragen:

Aus dem Vertragsrecht: Wer ist für Wartung/Reparatur verantwortlich? Erlaubt der Vertrag des Beschäftigten nur die private Nutzung oder ist auch die Nutzung für berufliche Zwecke zulässig?

Aus dem Steuerrecht bzw. hinsichtlich Kosten: Wie wird der Beschäftigte für die Nutzung seines privaten Gerätes entschädigt? Beteiligt sich der Arbeitgeber an den Kosten des Mobilfunkvertrages des Beschäftigten oder wird der Mobilfunkvertrag des Unternehmens genutzt? Ist hierbei eventuell ein geldwerter Vorteil zu versteuern?

Aus dem Haftungsrecht: Wer haftet bei Verlust oder Beschädigung des Gerätes während der beruflichen Tätigkeit? Nachdem für die Konstellation innerhalb eines BYOD-Modells noch keine Rechtsprechung zu existieren scheint, kann hier wohl vergleichend auf die Grundsätze des Bundesarbeitsgerichts zur Haftung bei der betrieblichen Nutzung eines privaten KFZ verwiesen werden, wonach eine Haftung des Arbeitgebers nach § 670 BGB analog in Betracht kommen würde. Es würde sich also anbieten, dass der Arbeitgeber eine Versicherung für das Gerät abschließt.

Arbeitsrechtliche Fragen

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

Einbeziehung der Arbeitnehmervertretung

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 der Betriebs-/Personalrat 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).

Sonderprobleme beim Einsatz eines MDM-Tools

Entscheidet sich das Unternehmen dafür, im Rahmen des BYOD-Modells – neben dem verschlüsselten Container (z.B. SecurePIM) – noch ein sog. Mobile-Device-Management (MDM)-Tool einzusetzen, so werden hierdurch weitreichende Zugriffs- und Einsichtnahmemöglichkeiten für das Unternehmen geschaffen, in die der Beschäftigte zusätzlich einwilligen muss. 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.

Darüber hinaus stellen sich hier Fragen hinsichtlich des Schutzes der Privatsphäre der Beschäftigten (v.a. des Rechtes auf informationelle Selbstbestimmung, Art. 2 Abs. 1, Art. 1 Grund-

BYOD
RECHTLICHE ASPEKTE

gesetz, GG) sowie Fragen hinsichtlich der Verletzung des Fernmeldegeheimnisses (§ 88 Telekommunikationsgesetz, TKG), wenn der Arbeitgeber eventuell Zugriff auf private E-Mails nehmen oder das private Sufverhalten überwachen kann.
Es ist dabei fraglich, ob es der Akzeptanz eines BYOD-Modells zuträglich ist, wenn sich die Beschäftigten ggf. vom Arbeitgeber „beobachtet“ fühlen, so dass eine Lösung ohne die Zuhilfenahme eines MDM-Tools vorzugswürdig scheint.

BEI DER EINFÜHRUNG EINES BYOD-MODELLS HINZUZUZIEHENDE STELLEN

Wie sich aus dem Obenstehenden ergibt, sind bei der Einführung eines BYOD-Modells folgende Stellen hinzuzuziehen:

+ IT-Abteilung: Sie muss die technischen Details klären und v.a. die Anwendungssoftware installieren bzw. die Beschäftigten bei der Installation unterstützen. Durch die Heterogenität der privaten Geräte ergibt sich ggf. ein höherer administrativer Aufwand.
+ HR-Abteilung: Sie muss die Mitarbeitervereinbarung unterzeichnen lassen und dann zur Personalakte nehmen.
+ Datenschutzbeauftragter: Er ist immer hinzuzuziehen, wenn personenbezogene Daten verarbeitet werden.
+ Abteilung Recht/Compliance: Sie muss die Mitarbeitervereinbarung erstellen und ggf. mit dem Betriebs-/Personalrat verhandeln.
+ Ggf. Betriebs-/Personalrat (§ 87 Abs. 1 Nr. 1, 2, 6 BetrVG) (von Beginn an): Falls ein solcher besteht, ist er von Beginn an einzubeziehen.

BEI DER EINFÜHRUNG EINES BYOD-MODELLS ZU ERSTELLENDE DOKUMENTE

+ Technische Dokumentation mit Freigabeformular: Hier sollte geregelt sein, mit welchem Gerät der Beschäftigte am BYOD-Modell teilnehmen möchte, wie die Installation abläuft und wer die Teilnahme genehmigt hat.
+ Wenn ein Betriebs-/Personalrat besteht: Betriebsvereinbarung: Hier können die allgemeinen Regelungen zur Nutzung der privaten Geräte im Rahmen des BYOD-Modells abgebildet werden, um eine Einheitlichkeit im Unternehmen herstellen zu können.
+ Nutzungsvereinbarung/Einwilligungserklärung: Nachdem der Betriebs-/Personalrat nicht über die privaten Geräte der Beschäftigten bestimmen kann, müssen die Mitarbeiter individuell ihre Bereitschaft zur Teilnahme am BYOD-Modell ausdrücken und die Regelungen anerkennen, sowie in die Datenverarbeitung einwilligen (wobei Art. 7 DSGVO zu beachten ist).

ZUSAMMENFASSUNG

Die Einfügung eines BYOD-Modells hat Vorteile. Die Beschäftigten können im Rahmen eines BYOD-Modells ihr eigenes, modernes Gerät, das sie kennen, für die betriebliche Nutzung verwenden. Das bedeutet:

+ Mitarbeiter müssen nur ein Gerät mitführen
+ Steigerung der Produktivität und der Erreichbarkeit
+ Sinkender Schulungsbedarf
+ Erhöhung der Zufriedenheit der Beschäftigten
+ Bessere Identifikation mit dem Arbeitgeber
+ Geringere Anschaffungskosten für den Arbeitgeber

Gleichzeitig müssen auch zahlreiche rechtliche Herausforderungen eines BYOD-Modells gelöst werden:

+ Verwaltung der unterschiedlichen Mobilgeräte (daher Beschränkung auf bestimmte Hersteller anzuraten)
+ Abdeckung aller rechtlichen Aspekte (soweit möglich) durch Betriebsvereinbarungen und Mitarbeitervereinbarungen/Einwilligungserklärungen
+ Ausräumung von Bedenken hinsichtlich Zugriffsmöglichkeiten des Arbeitgebers auf private Daten (Fotos, E-Mails, usw.), falls ein MDM-Tool zum Einsatz kommt

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 von Seiten der Beschäftigten an die Unternehmensleitung herangetragen, so dass diese Voraussetzung erfüllt ist.

BYOD
RECHTLICHE ASPEKTE

Durch die Verwendung einer entsprechenden Anwendungssoftware und durch den Abschluss entsprechender Vereinbarungen (Mitarbeitervereinbarung/Einwilligung und gegebenenfalls Betriebsvereinbarung) können die Vorteile für Beschäftigte und Unternehmen optimal genutzt und die rechtlichen Herausforderungen gelöst werden.

Von dem Einsatz von privater Technik für berufliche Belange ohne ein BYOD-Modell und ohne die hier beschriebenen technischen und organisatorischen Regelungen muss in jedem Fall abgeraten werden, da sich hierdurch erhebliche Risiken ergeben. Mit der Geltung der Datenschutzgrundverordnung (DSGVO) ab Mai 2018 wird sich dabei v.a. auch das Bußgeldrisiko, das bei einer Verletzung des Datenschutzrechts droht, erheblich vergrößern, da hierin Bußgelder von bis zu 20 Millionen Euro bzw. 4% des gesamten weltweiten Jahresumsatzes vorgesehen sind.

HEUSSEN Rechtsanwaltsgesellschaft mbH

Die Lösung:
SecurePIM - Sicher Mobil Arbeiten

Die Anwendungssoftware SecurePIM kann vor allem die folgenden Aspekte der rechtlichen Herausforderungen abdecken:

- ✓ Strikte Trennung der privaten von den beruflichen Daten, u.a. direkte Speicherung von Fotos von der Kamera des Gerätes in den verschlüsselten Container (ohne Zwischenspeicherung auf dem privaten Gerät)
- ✓ Verschlüsselte Aufbewahrung der Daten auf dem Gerät
- ✓ Möglichkeit der Fernlöschung für den Arbeitgeber
- ✓ Verschlüsselte Übertragung vom Server in den verschlüsselten Container auf dem Gerät
- ✓ Verschlüsselte Versendung von E-Mails

ÜBER VIRTUAL SOLUTION AG

Virtual Solution hat es sich zur Aufgabe gemacht Sicherheit und Benutzerfreundlichkeit in der mobilen Arbeitswelt der Zukunft zu verbinden. Bereits seit 1996 entwickelt und vertreibt das deutsche Unternehmen Sicherheitslösungen, die auf die Sicherheitsbedürfnisse einer zunehmend digitalisierten und mobilen Gesellschaft zugeschnitten sind.

Virtual Solution AG
Blutenburgstraße 18
D-80636 München

+49 (0)89 30 90 57-0

kontakt@virtual-solution.com
www.virtual-solution.com