Mobile Geräte DSGVO-konform verwalten

Enterprise Mobility Management und die EU-Datenschutzgrundverordnung

Der digitale Wandel ist überall und ergreift Wirtschaft und Gesellschaft. In der Folge steigt die Menge an Daten, die über das Internet ausgetauscht werden, beständig an – darunter auch sogenannte personenbezogene Daten, die Informationen über einzelne Personen enthalten und potenziell Rückschlüsse über diese zulassen.

Firmen weltweit sammeln diese Daten, um daraus wertvolle Erkenntnisse über das Verhalten ihrer Kunden für Geschäftsentscheidungen zu gewinnen. Der einfache Datenaustausch zwischen den Ländern der Europäischen Union war deshalb auch eines der Ziele, die das Europäische Parlament mit seiner Verordnung zur europäischen Datenschutzgrundverordnung verbindet.

Demgegenüber hatte sich schon seit geraumer Zeit – nicht nur in Europa – die Auffassung durchgesetzt, dass die Auswertung von Daten bestimmter Personen immer als Eingriff in deren Persönlichkeitssphäre zu verstehen ist. Im Sinne der persönlichen Freiheit und Selbstbestimmung der EU-Bürger – wie sie auch zahlreiche europäische Verfassungen festschreiben – hat deshalb jedes Individuum das uneingeschränkte Recht, selbst über die Verwendung seiner Daten zu entscheiden.

In der alltäglichen Praxis des Datensammelns und -verarbeitens rückte dieses Recht jedoch oftmals zugunsten von Unternehmensinteressen in den Hintergrund. Mit der DSGVO will die EU den Verbrauchern nun die Hoheit über ihre persönlichen Daten zurückgeben, ein einheitliches Datenschutzniveau einführen und eine EU-weite rechtliche Grundlage für das digitale Zeitalter legen.

APPTEC360
Unified Endpoint Management

Freie Strasse 32
CH - 4001 Basel
Switzerland

Phone: +41 (0) 61 511 32 10
Telefax: +41 (0) 61 511 32 19
eMail: info@apptec360.com

Mit EMM Kontrolle über mobile Geräte behalten

Unternehmen, die die strengen Vorgaben des neuen Regelwerkes nicht einhalten, müssen mit empfindlichen Bußgeldern rechnen. Bei Verstößen gegen die Verordnung drohen Geldstrafen in Höhe bis zu 20 Millionen Euro oder bis zu vier Prozent des globalen Gesamtumsatzes. – je nach dem welcher Wert der höhere ist.

Personenbezogene Daten entstehen an vielen Stellen im Unternehmen, darunter auch bei der Verwaltung mobiler Geräte, die unter dem Schlagwort „Mobility First“ zunehmend die Business-Welt erobern. Alle Daten, die Informationen etwa über das verwendete Gerät in Verbindung mit den persönlichen Daten zum Beispiel eines Mitarbeiters, Kunden oder Dienstleisters enthalten, fallen unter die DSGVO und sind entsprechend zu schützen. Ein Enterprise-Mobility-Management-System (EMM) kann Unternehmen die dafür notwendige umfassende Kontrolle über Daten, Apps und Geräte verschaffen und so eine zentrale Komponente zur Einhaltung der DSGVO darstellen.

In diesem Dokument erfahren Sie, welche Grundsätze der DSGVO zugrunde liegen und welche Auswirkungen diese auf das EMM haben. Dieses Dokument stellt keine Rechtsberatung dar. Jedes Unternehmen muss sicherstellen, dass der Betrieb einer EMM-Plattform rechtskonform und gemäß interner Compliance-Vorgaben erfolgt.

Grundsätze der DSGVO: Die wichtigsten Aussagen und Vorgaben

Die Digitalisierung durchdringt zunehmend alle Bereiche des menschlichen Lebens wie auch der Wirtschaft. Personenbezogene Daten sind deshalb zwangsläufig in jedem Unternehmen zu finden. Um diese Daten einheitlich und effizient zu schützen, stellt die DSGVO deshalb gleich zu Beginn in Artikel 5 ihres Regelwerkes klar, welchen Grundsätzen eine rechtskonforme Datenverarbeitung in Unternehmen folgen muss. Firmen, die die Datenverarbeitung dabei ganz oder teilweise an einen Dienstleister übergeben – der so genannte Auftragsverarbeiter – tragen gemeinsam mit diesem die Verantwortung für die Einhaltung der Datenschutzvorgaben.

- **Transparenz:** Die Datenverarbeitung muss nicht nur rechtmäßig und nach Treu und Glauben erfolgen, sondern auch für die betroffene Person nachvollziehbar sein. Einzelpersonen haben ein Recht, sich über die Datenspeicherung zu informieren.
- **Zweckbindung:** Daten dürfen nur zu dem Zweck verwendet werden, für den sie auch erhoben wurden.
- **Datensparsamkeit:** Die Datenerhebung muss dabei so erfolgen, dass sie dem Zweck angemessen ist, sie darf nur relevante Daten umfassen und das notwendige Maß nicht überschreiten.
- **Genauigkeit:** Personenbezogene Daten müssen sachlich richtig und aktuell sein. Unrichtige Daten müssen unverzüglich gelöscht oder berichtig werden.
- **Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für den erwünschten Zweck erforderlich ist.
- **Datensicherheit und -schutz:** Unternehmen sind dazu verpflichtet, Daten sicher zu verarbeiten, um sie beispielweise vor unbefugter Nutzung oder Verlust zu schützen.
- **Dokumentation:** Unternehmen müssen die Einhaltung der genannten Grundsätze nachweisen können. Dies zieht umfassende Dokumentationspflichten nach sich.

Rechtskonformes Mobility Management von Anfang an

Datenschutz beginnt im Sinne der europäischen Gesetzgeber nicht erst mit dem Prozess der Datenverarbeitung, sondern bereits mit den Rahmenbedingungen, unter denen die Nutzung von Informationen im Unternehmen erfolgt. Die DSGVO verpflichtet Organisationen in Artikel 25, durch Technik (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default), die Einhaltung der genannten Grundprinzipien sicherzustellen.

Privacy by Design
Firmen müssen diejenigen technischen Maßnahmen etablieren, die erforderlich sind, um den geforderten Datenschutz umzusetzen.

Privacy by Default
Außerdem müssen Produkte und Dienstleistungen so voreingestellt sein, dass nur Daten erhoben werden, die für die Nutzung des Produkts oder der Dienstleistung notwendig sind. Das Datensammeln auf Vorrat verbietet sich damit. Außerdem hat der Nutzer die Möglichkeit, diese Einstellungen im Nachhinein jederzeit zu verändern.

Verarbeitung auf dem Stand der Technik
Um einen höchstmöglichen Standard bei der Datensicherheit zu gewährleisten, geht die DSGVO in Artikel 32 noch einen Schritt weiter: Danach müssen die für den Datenschutz geeigneten technischen und organisatorischen Maßnahmen dem aktuellen Stand der Technik entsprechen. Artikel 32 zählt explizit Verschlüsselung, Recovery, die Verfügbarkeit und Belastbarkeit von Systemen sowie weitere Bereiche auf, für die das State-of-the-Art-Kriterium gilt.

Personenbezogene Daten mit EMM schützen

Als technisches Tool im Sinne der DSGVO kann eine EMM-Lösung maßgeblich zu einem effektiven Datenschutz im Bereich Mobility Management beitragen. Sie verschafft Unternehmen die umfassende Kontrolle über Daten, Apps und Geräte – und mit dem umfassenden Einsatz solcher Lösungen ist eine wichtige Voraussetzung zur Erfüllung des By-Design- wie auch des State-of-the-Art-Prinzips gegeben.

Angesichts der zunehmenden Bedeutung mobiler Geräte in Unternehmen, werden diese umgekehrt in Erklärungsnot geraten, wenn sich im Falle einer Datenschutzverletzung herausstellt, dass Maßnahmen nach dem neuesten Stand der Technik – etwa im Rahmen eines effektiven Einsatzes von EMM – ausgeblieben sind.

Mit AppTec als EMM-Lösung lassen sich die Grundsätze der EU-Datenschutzgrundverordnung wie folgt umsetzen:

- **Die Plattform** stellt die Trennung privater von geschäftlichen Daten – wie E-Mail, Kontakte usw. – anhand von Container-Technologie sicher. AppTec setzt dabei für alle iOS- und Android-Geräte auf eine Container-Technologie, mit dem sich ein sicherer Bereich auf dem Gerät erstellen lässt. Weder andere Anwendungen, noch andere Systeme oder nicht autorisierte Personen erhalten Zugang zu den Daten im Container.
- **Der IT-Administrator** hat stets die volle Kontrolle darüber, welche Geräte, Apps und Personen auf Geschäftsdaten zugreifen und kann dies per Audit-Protokoll jederzeit nachweisen. So gestattet das Mail-Gateway der AppTec EMM nur autorisierten Geräten mit hinterlegter Seriennummer den Zugriff auf Firmendaten. Auf diese Weise lässt sich die Verbreitung von Daten auf firmenfremden Geräte (etwa von Familienmitgliedern oder Freunden) unterbinden.
- **Mit der EMM-Plattform** lässt sich die gesamte Kommunikation mit dem Firmenserver über Firmen-Apps – wie z.B. SAP-Apps auf dem Smartphone oder Tablet – verschlüsseln. Über die VPN-Schnittstelle des AppTec Universal Gateway können Unternehmen Firmengeräte vollautomatisch und sicher mit dem Firmennetzwerk verbinden und sogar den Zugang auf gewünschte Firmen-Apps beschränken.
- **Die AppTec EMM-Plattform** stellt die Einhaltung der Compliance-Richtlinien des Unternehmens sicher, indem … *(weiter auf Seite 4)*

“Produkte und Dienstleistungen müssen so voreingestellt sein, dass nur Daten erhoben werden, die für die Nutzung des Produkts oder der Dienstleistung notwendig sind.”

Die AppTec EMM-Plattform *stellt die Einhaltung der Compliance-Richtlinien des Unternehmens sicher, indem …*

- ... sich bestimmte Sicherheitskonfigurationen für Geräte und Anwendungen voreinstellen lassen, wie zum Beispiel Richtlinien zur Passworterstellung oder Optionen zur Verschlüsselung des Gerätes im Verlustfall (Data Loss Prevention – DLP). Mittels Whitelist können Apps darüber hinaus auf eine zur Nutzung freigegebene Positivliste beschränkt bzw. mittels Blacklist über eine Negativliste von der Nutzung ausgeschlossen werden.
- … sie diese automatisch überwacht und Angriffe auf die Integrität des Betriebssystems durch eine Manipulation dieses Systems (Jailbreak oder Root) erkennen kann.
- … sie im Fall eines externen Angriffs eine umfassende Sicherheitsregie in Gang setzt (Compliance and Escalation): Ein Verstoß der Compliance-Vorgaben wird zunächst erfasst und identifiziert (Schritt1, z. B. Gerät meldet sich nicht), die Folgemaßnahme wird ausgelöst (Schritt 2, z. B. Gerät in Quarantäne stellen) und der Administrator informiert (Schritt 3).

Wege zu einem DSGVO-konformen EMM

Um Klarheit über den Anpassungsbedarf beim Mobility Management im eigenen Unternehmen zu gewinnen, kann zunächst eine Gap-Analyse durchgeführt werden. Dabei wird in einem ersten Schritt geprüft, welche Vorgaben der Verordnung durch aktuelle Prozesse und Konfigurationen bereits erfüllt werden. Im zweiten Schritt wird ermittelt, wo Nachholbedarf besteht.

Generell sollten Firmen mit ihrem EMM folgende Aufgaben und Prozesse abdecken, um mobile Geräte DSGVO-konform verwalten und steuern zu können:

- **unternehmensweite Verwaltung** aller Mobilgeräte, die Zugriff auf Unternehmensdaten haben und Sperren aller Geräte, Apps und Benutzer die nicht vom EMM erfasst und autorisiert sind
- **Vorgabe von Richtlinien** etwa zur Erstellung von Passwörtern oder zur Vermeidung von Datenverlust (DLP-Richtlinien) sowie zur Nutzung vertrauenswürdiger Datenübertragungswege wie VPN
- **effektives Mobile App Management** über einen eigenen „Enterprise App Store“, der die ganzheitliche Kontrolle von Apps über den gesamten Lebenszyklus ermöglicht
- **Erstellen klarer und zentraler Richtlinien** zum Datenschutz für alle Nutzer mobiler Geräte
- **Sensibilisieren von Führungskräften** für EMM-Neuerungen durch die DSGVO und Kommunikation gegenüber den Mitarbeitern unter anderem im Rahmen von Schulungen
- **klare Prozesse** für die Herausgabe von Personendaten auf Wunsch des Besitzers
- **Dokumentation aller relevanten EMM-Maßnahmen** in Protokollen und Audits sowie klare Prozesse beim Auftreten eines Sicherheitsvorfalls (inklusive Meldepflicht)

FAZIT:

Sicherheit und Schutz personenbezogener Daten, die rund um die Verwaltung mobiler Geräte in einem Unternehmen entstehen, lassen sich nur auf Basis einer zuverlässigen, sicherheitszentrierten und bedienerfreundlichen Enterprise-Mobility-Management-Lösung realisieren. AppTec360 Enterprise Mobility Management setzt als umfassende „Mobility First“-Lösung Datensicherheit an erste Stelle. Gefahren des Datenverlusts setzt AppTec360 einen Schutzwall integrierter Maßnahmen und Sicherungsoptionen entgegen. Unternehmen setzen bei AppTec im ansonsten angloamerikanisch dominierten Markt überdies auf einen einzigartigen Vorteil: Die Software des Schweizer Anbieters wird ausschließlich in der Schweiz entwickelt, seine Server sind in Deutschland und der Schweiz positioniert und vor dem Zugriff transatlantischer Institutionen geschützt.

Im Unternehmensalltag stellt die Handhabung eines herkömmlichen EMM Systems mit fortwährend erweitertem Funktionsumfang für IT Administratoren längst eine Herausforderung dar. Dies kann eine effiziente Nutzung des Mobility Managers einschränken – und damit die Einhaltung der DSGVO-Grundsätze erschweren. Ganz anders bei AppTec360. Das Design des AppTec360 Dashboards ist konsequent auf intuitive Bedienbarkeit ausgerichtet und einzigartig praxisnah.

Haftungsausschluss:

Wir machen darauf aufmerksam, dass dieses Dokument nur dem unverbindlichen Informationszweck dient. Es stellt weder eine Rechtsberatung noch ein Rechtsgutachten dar. Dieses Dokument begründet auch keine Beziehung zwischen Rechtsbeistand und Client. Sein Inhalt kann und soll eine verbindliche Rechtsberatung nicht ersetzen, die die spezifische Situation in Ihrem Unternehmen berücksichtigt. Klären Sie konkrete Rechtsfragen in jedem Fall mit Ihrem Anwalt. AppTec übernimmt weder eine Haftung noch eine Verantwortung für Schäden, die aus oder im Zusammenhang mit der Verwendung dieses Dokuments entstehen.

APPTEC360
Unified Endpoint Management

Freie Strasse 32
CH - 4001 Basel
Switzerland

Phone: +41 (0) 61 511 32 10
Telefax: +41 (0) 61 511 32 19
eMail: info@apptec360.com