EMM – ein nützliches Werkzeug zur Einhaltung der DSGVO

Angemessene, auf dem gesunden Menschenverstand basierende Sicherheitsstandards erlangen in vielen Regionen der Welt Gesetzeskraft. In Europa gilt ab 25. Mai 2018 die im April 2016 verabschiedete „Datenschutz-Grundverordnung" in vollem Umfang. Mit der Datenschutz-Grundverordnung wird für die Europäische Union (EU) ein umfassendes und harmonisiertes Rechtssystem für Datenschutz und Datensicherheit eingeführt. Bei Nichteinhaltung der Datenschutz-Grundverordnung drohen erhebliche Geldstrafen und ein Imageschaden – die Höchststrafen liegen bei über 20 Mio. Euro bzw. 4 % des weltweiten Ertrags des Unternehmens.

Die Datenschutz-Grundverordnung gilt für die für die Verarbeitung Verantwortlichen und Auftragsverarbeiter in der EU sowie außerhalb der EU, wenn diese personenbezogene Daten von Personen aus der EU verarbeiten. Ein „für die Verarbeitung Verantwortlicher" ist das Unternehmen, das über den Zweck und

MobileIron

info@mobileiron.com
www.mobileiron.com
Tel.: +1 877 819 3451
Fax :+1.650.919.8006

„EMM-Plattform in Zukunft unverzichtbar für die Einhaltung der Datenschutz-Grundverordnung“

IDC (Februar 2017)*

die Mittel der Verarbeitung personenbezogener Daten entscheidet. „Auftragsverarbeiter“ ist jedes Unternehmen, das die Verarbeitung im Namen und entsprechend den Weisungen des für die Verarbeitung Verantwortlichen übernimmt. Bei diesem Dokument gehen wir davon aus, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter identisch sind, das heißt, dass es sich um ein Unternehmen mit Mitarbeitern oder Kunden in der EU handelt.

Ein umfassendes und gut strukturiertes Enterprise Mobility Management-Programm (EMM) wird ein wichtiger Bestandteil der Initiative zur Einhaltung der DS-GVO jedes Unternehmens sein. In diesem Dokument finden Unternehmen Rahmenbedingungen, mit denen sie ihre Richtlinien für mobilen Datenschutz und mobile Sicherheit sowie die Durchsetzungskonzepte bewerten können. Dieses Dokument stellt keine Rechtsberatung dar. Jedes Unternehmen muss sicherstellen, dass die Einführung einer EMM-Plattform sich in seine internen juristischen und Compliance-Rahmenbedingungen einfügt.

Die Grundsätze für die Verarbeitung personenbezogener Daten nach der Datenschutz-Grundverordnung DS-GVO basieren auf Standards und stimmen mit den entstehenden Datenschutzbestimmungen in anderen Regionen überein.

Grundsätze der Datenschutz-Grundverordnung

Jeder Arbeitgeber besitzt bestimmte personenbezogene Daten. Ausgangspunkt für die Datenschutz-Grundverordnung ist die einfache Überlegung, dass nur die unbedingt erforderlichen personenbezogenen Daten gespeichert werden sollen und angemessene Vorsichtsmaßnahmen zur Risikominderung für Einzelpersonen ergriffen werden müssen.

Zwar ist Europa in der Welt im Bereich des Datenschutzes führend, die Grundsätze zur Verarbeitung personenbezogener Daten entsprechend der Datenschutz-Grundverordnung basieren jedoch auf Standards und stimmen mit den entstehenden Datenschutz-Rahmenbedingungen in anderen Regionen überein. Diese Grundsätze sind:

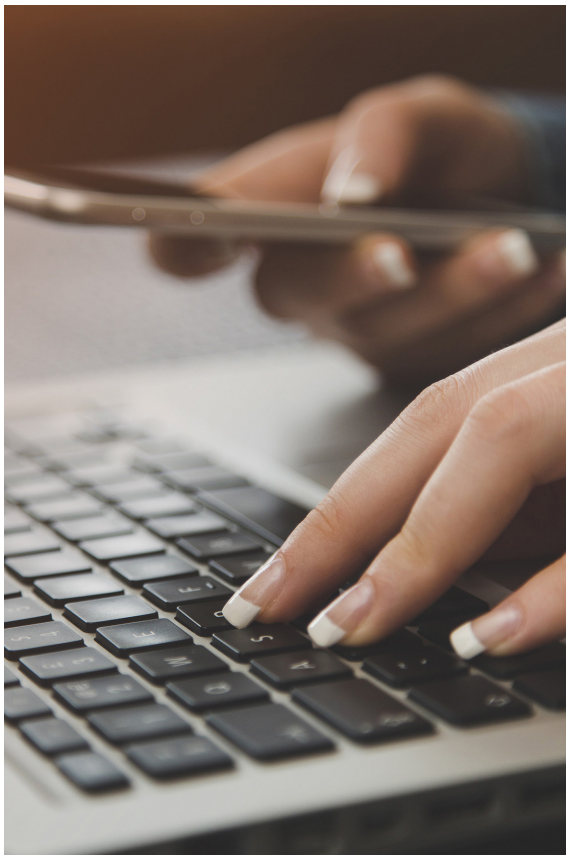
- **Gesetzeskonforme, angemessene und transparente Verarbeitung:** Unternehmen müssen triftige Gründe für die Verarbeitung personenbezogener Daten haben und diese Informationen Einzelpersonen zur Verfügung stellen.
- **Es muss einen klaren und expliziten Grund für die Verarbeitung der personenbezogenen Daten geben.** Die Daten dürfen nur für den Zweck verarbeitet werden, für den sie erfasst wurden.
- **Zustimmung:** Die natürliche Person, deren personenbezogene Daten verarbeitet werden, muss der Verarbeitung allgemein zustimmen.
- **Datensparsamkeit:** Die verarbeiteten Daten sollten auf den Umfang begrenzt sein, der für einen bestimmten Zweck unbedingt benötigt wird. Zugang darf nur den Personen gewährt werden, die sie für den betreffenden Zweck benötigen.
- **Genauigkeit:** Die Daten sollten korrekt sein, Fehler sollten sich leicht beseitigen lassen. Natürliche Personen sollten das Recht haben, eine Korrektur dieser Daten zu verlangen.

* "Marktanalyse-Pespektive: Unternehmensmobilität in Westeuropa 2017", von IDC Europa, Februar 2017.

- **Speicherbegrenzung:** Die Daten sollten nur so lange aufbewahrt werden, wie sie für den angegebenen Zweck benötigt werden.
- **IT-Sicherheit:** Die Daten müssen so verarbeitet werden, dass eine angemessene Datensicherheit gewährleistet ist, beispielsweise ein Schutz vor Verarbeitung durch Unbefugte und versehentlichen Verlust.
- **Rechenschaftspflicht:** Das Unternehmen muss die Einhaltung der Compliance und die Berücksichtigung der oben erwähnten Grundsätze nachweisen können.

Ein Unternehmen muss nachweisen können, dass es angemessene Sicherheitsmaßnahmen implementiert hat und die Compliance entsprechend überwacht wird.

Datenschutz lässt sich nicht im Nachhinein einführen.



Privacy by Design und Privacy by Default – Artikel 25 der DSGVO

Datenschutz lässt sich nicht im Nachhinein einführen. Artikel 25 der Datenschutz-Grundverordnung definiert das „Konzept des Datenschutzes nach Design und nach Standard", auch bekannt als „Privacy by Design and by Default".

Datenschutz nach Design: Das Unternehmen muss den Datenschutz während des gesamten Arbeitszyklus sicherstellen, von der Erstverarbeitung und dem Systemkonzept bis zum Ende der Nutzungsdauer und der Datenlöschung.

Datenschutz nach Standard: Das Unternehmen muss standardmäßig sicherstellen, dass nur die benötigten personenbezogenen Daten erfasst und verarbeitet werden. Der Benutzer soll die Abfrage zusätzlicher Informationen nicht erst verweigern müssen. Das Unternehmen darf keine weiteren Informationen sammeln, nur weil es sie später benötigen könnte.

Stand der Technik – Artikel 32 der Datenschutz-Grundverordnung

Artikel 32 der Datenschutz-Grundverordnung unterstreicht die Bedeutung der Verwendung der aktuellen, jeweils besten Technologien zur Unterstützung der Information Governance:

*„Unter Berücksichtigung des **Standes der Technik** ... müssen der für die Verarbeitung Verantwortliche und der Datenauftragsverarbeiter geeignete technische und organisatorische Maßnahmen implementieren, um eine dem Risiko angemessene Sicherheit zu gewährleisten."*

Obgleich die Datenschutz-Grundverordnung keine spezifischen technischen Implementierungen vorschreibt, erwähnt Artikel 32 Verschlüsselung, Datenintegrität, Verfügbarkeit und Tests als Beispiele für Maßnahmen, mit denen das Unternehmen Lösungen nach dem neuesten Stand der Technik prüfen sollte.

EMM-Rahmenbedingungen für die Datenschutz-Grundverordnung

EMM-Lösungen, beispielsweise die Lösung von MobileIron, sind eine wichtige Komponente eines Sicherheitsprogramms zur Einhaltung der Datenschutz-Grundverordnung. Einem Unternehmen, das EMM nicht effektiv einsetzt, wird es gegenüber den Behörden schwer fallen zu begründen, weshalb es keine Maßnahmen nach dem neusten Stand der Technik einsetzte, um die Gefahr von Datenverlust zu reduzieren.

Einem Unternehmen, das EMM nicht effektiv einsetzt, wird es gegenüber den Behörden schwer fallen zu begründen, weshalb es keine Maßnahmen nach dem neusten Stand der Technik einsetzt.

Eine EMM-Plattform zur Einhaltung der Datenschutz-Grundverordnung muss folgende Funktionen von MobileIron einschließen:

1. Mit der Plattform von MobileIron kann das Unternehmen eine **Datenverschlüsselung** auf dem Gerät durch Überwachung der Verschlüsselungseinstellungen für das Gerät erzwingen und eine sekundäre Verschlüsselung für Unternehmens-Apps und Unternehmensdaten anbieten.
2. Mit der Plattform von MobileIron kann das Unternehmen eine **klare Grenze zwischen privaten und Unternehmensdaten** auf dem Gerät definieren. Das Unternehmen muss dazu keinen Zugriff auf den Content der privaten Apps bzw. der privaten E-Mail-Konten haben. Jedes Unternehmen muss außerdem prüfen, ob der Zugriff auf andere Arten personenbezogener Daten, beispielsweise ein App-Verzeichnis oder den Gerätestandort, aus betrieblichen oder Sicherheitsgründen notwendig ist. Wenn dies der Fall ist, sollte diese Notwendigkeit klar definiert und kommuniziert werden. Die entsprechenden Datenschutz- und Zustimmungsmaßnahmen müssen dann proaktiv implementiert werden.
3. Mit der Plattform von MobileIron kann das Unternehmen einen **vertrauenswürdigen Zugriff auf Unternehmensdienste erzwingen.** Mit MobileIron Access wird für das Unternehmen transparent, welche Mobilgeräte und Apps eine Verbindung mit Backend-Diensten aufbauen wollen. Zugriffsversuche Unbefugter können dann gesperrt werden. MobileIron Sentry schützt den Daten-Traffic und kann diesen ggf. auch über zusätzliche Sicherheits- und Inspektionsgateways umleiten.
4. Mit der Plattform von MobileIron kann das Unternehmen **anhand der Audit-Protokolle** erkennen, welche Aktionen zu einer Datensicherheitslücke führten und welche Gegenmaßnahmen gegebenenfalls ergriffen wurden. In bestimmen Situationen beträgt die gesetzlich vorgeschriebene Meldefrist entsprechend der Datenschutz-Grundverordnung nur 72 Stunden, das heißt, es muss schnell reagiert werden.
5. Die Plattform von MobileIron ermöglicht es dem Unternehmen, **Kontrollen zur Vermeidung von Datenverlusten (DLP) zu erzwingen.** Mit diesen Kontrollen kann das Unternehmen vertrauliche Daten auf einem verloren gegangenen Gerät löschen aus der Ferne und sicherstellen, dass Unternehmens-Apps auf einem Gerät keine Daten mit nicht autorisierten Apps teilen. Diese Kontrollen können außerdem Angriffe auf die Integrität des mobilen Betriebssystems durch Jailbreaking oder Rooting erkennen. Wenn die Compliance nicht mehr gewährleistet ist, kann das Unternehmen mit der Plattform von MobileIron entsprechende Gegenmaßnahmen einleiten, beispielsweise eine Benachrichtigung senden, das Gerät in Quarantäne stellen oder Daten löschen.

Mit nicht verwalteten Mobilgeräten lässt ich keine solide Abwehrstrategie aufbauen

EMM für die Datenschutz-Grundverordnung

Jedes Unternehmen, das die Datenschutz-Grundverordnung berücksichtigen muss, sollte seine EMM-Implementierung und Konfiguration überprüfen. Durch die Prüfung werden einmal Lücken identifiziert, wenn nicht alle Funktionen der EMM-Plattform genutzt werden und die Plattform nicht alle Anforderungen der Datenschutz-Grundverordnung erfüllt. Zweitens ist damit das Fundament für den Entwurf und die Implementierung eines Programms zur laufenden Überwachung der Compliance und zur Einleitung von Gegenmaßnahmen geschaffen.

Dies ist der Ausgangspunkt, um eine EMM-Plattform als Teil eines mit der Datenschutz-Grundverordnung kompatiblen Sicherheitsprogramms bereitzustellen.

1. Sorgen Sie dafür, dass alle Mobilgeräte verwaltet werden, wenn diese Zugriff auf Unternehmensdaten haben. Mit nicht verwalteten Mobilgeräten lässt sich keine umfassende, tiefe Verteidigungsstrategie umsetzen und der Datenschutz bei verloren gegangenen oder gefährdeten Geräten nicht angemessen gewährleisten.
2. Verwenden Sie aktuelle Konfigurationsprofile. Erzwingen Sie Richtlinien für Passwörter, Verschlüsselung, Gerätesicherheit, Konnektivität und andere, für das Unternehmen relevante Aktivierungsfunktionen.
3. Verteilen Sie alle Unternehmens-Apps als verwaltete Apps über einen Unternehmens-App-Store, sodass diese Apps in dem vom Unternehmen kontrollierten Sicherheitsrahmen funktionieren.
4. Erzwingen Sie Richtlinien zur Vermeidung von Datenverlusten (DLP-Richtlinien) zum Schutz der App-Daten auf dem Gerät.
5. Erzwingen Sie für alle Unternehmensdienste einen vertrauenswürdigen Zugang. Sperren Sie den Zugriff für nicht autorisierte, nicht verwaltete oder nicht kompatible Geräte, Apps und Benutzer. Lassen Sie nicht zu, dass vertrauliche Daten auf einem Gerät gespeichert werden, das für das Unternehmen nicht transparent ist und nicht kontrolliert wird.
6. Definieren und kommunizieren Sie gegenüber den Mitarbeitern regelmäßig klar die Richtlinien für Datenschutz und Sicherheit.
7. Erfassen Sie in geeigneten Protokollen Bestand, Nutzung und Audits, damit Sie bei einer Sicherheitslücke schnell reagieren können.

Fazit

Ein Unternehmen kann nur dann eine angemessene Sicherheit von personenbezogenen Daten gewährleisten, wenn es nachweisen kann, dass es entsprechende EMM-Kontrollen und Prozeduren implementiert hat. Diese sollten sicherstellen, dass die vom Unternehmen benötigten personenbezogenen Daten vor externen Bedrohungen sowie Verwendung oder Offenlegung durch Unbefugte geschützt sind. Die Plattform von MobileIron bietet robuste Rahmenbedingungen für die Einhaltung der Compliance durch Grundsätze wie Datensparsamkeit, Datenintegrität, Geheimhaltung sowie Verantwortlichkeit entsprechend den DSGVO-Bestimmungen.