# Perché una soluzione EMM può essere utile ai fini della conformità al GDPR

Alcuni standard di sicurezza ragionevoli, dettati dal buon senso, stanno diventando legge in molti paesi del mondo. In Europa, il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation), emanato nell'aprile 2016, verrà applicato a partire dal 25 maggio 2018. Il GDPR si prefigge di instaurare in tutta l'Unione Europea (UE) un unico regime legale completo e armonizzato in materia di protezione e riservatezza dei dati. Le sanzioni monetarie e i danni alla reputazione derivanti dalla mancata conformità al GDPR sono considerevoli: la sanzione massima corrisponde alla cifra più alta tra 20 milioni di euro e il 4% del fatturato globale dell'azienda.

Il GDPR si applica ai titolari e ai responsabili del trattamento dei dati all'interno e anche all'esterno dell'UE, se i dati personali trattati appartengono a soggetti dell'UE. Per "titolare del

MobileIron

info@mobileiron.com
www.mobileiron.com
Tel.: +1.877.819.3451
Fax: +1.650.919.8006

*"Una soluzione EMM diventa di importanza cruciale ai fini della conformità al GDPR".*

**IDC (febbraio 2017)***

trattamento" si intende l'organizzazione che decide lo scopo dell'elaborazione dei dati personali e i mezzi da utilizzare. Per "responsabile del trattamento" si intende l'organizzazione che gestisce l'elaborazione dei dati per conto del titolare o ne segue le istruzioni. Ai fini del presente documento, si presuppone che titolare e responsabile coincidano, ovvero che siano un'azienda con dipendenti o clienti nell'UE.

Un programma di gestione dell'enterprise mobility (EMM, Enterprise Mobility Management) completo e ben strutturato costituisce un elemento importante nell'ambito di un'iniziativa per la conformità al GDPR di un'azienda. Questo documento fornisce un quadro della situazione per le aziende che desiderano valutare in maniera proattiva le proprie policy sulla sicurezza e la privacy dei dispositivi mobili, nonché i relativi modelli di applicazione. Non deve essere inteso come guida di carattere legale. Ogni azienda deve garantire che l'implementazione EMM si integri in modo corretto con il proprio contesto legale e di conformità interno.

*I principi stabiliti dal GDPR per l'elaborazione dei dati personali sono basati su standard e coerenti con i contesti normativi emergenti in altre regioni in materia di privacy.*

## Principi del GDPR

Tutti i datori di lavoro sono in possesso di dati personali. Un punto di partenza sensato per la conformità al GDPR è gestire la quantità minima indispensabile di dati personali e adottare precauzioni ragionevoli per ridurre i rischi per le persone.

Sebbene l'Europa sia la prima al mondo a focalizzarsi sulla riservatezza dei dati, i principi di elaborazione dei dati personali recepiti in conformità al GDPR sono basati su standard e coerenti con altri contesti normativi emergenti in materia di privacy in altre zone. Questi principi includono quanto segue:

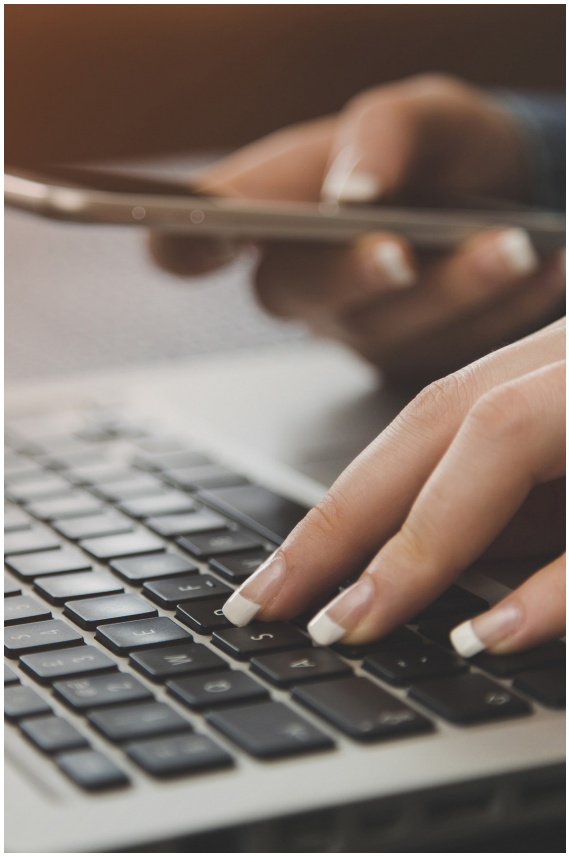
- **Elaborazione dei dati corretta, legale e trasparente:** le aziende devono avere motivazioni valide per elaborare dati personali e devono rendere disponibili tali informazioni ai soggetti interessati.
- **Limitazione dello scopo:** il motivo dell'elaborazione dei dati personali deve essere chiaro ed esplicito. I dati possono essere elaborati esclusivamente per il fine per il quale sono stati raccolti.
- **Consenso:** il soggetto a cui appartengono i dati da elaborare deve generalmente fornire il consenso.
- **Riduzione al minimo dei dati:** i dati elaborati devono essere limitati a quelli strettamente necessari per lo scopo specifico. L'accesso deve essere consentito esclusivamente alle persone che devono accedervi per lo scopo specificato.
- **Accuratezza:** i dati devono essere accurati ed eventuali imprecisioni devono poter essere corrette facilmente. I soggetti devono avere il diritto di richiedere eventuali rettifiche.

* "Market Analysis Perspective: Western Europe Enterprise Mobility, 2017" di IDC Europe, febbraio 2017.

- **Limitazione del periodo di archiviazione:** i dati devono essere conservati solo per il periodo necessario per lo scopo identificato.
- **Integrità e riservatezza:** i dati devono essere elaborati in modo da garantirne un'adeguata sicurezza, proteggendoli anche dalla perdita accidentale e dal trattamento non autorizzato.
- **Responsabilità:** l'azienda deve essere in grado di dimostrare la conformità ai suddetti principi e la capacità di rimediare.

Un'azienda deve essere in grado di dimostrare che ha messo in pratica misure di sicurezza adeguate e che monitora adeguatamente la conformità.

*La privacy non dev'essere un pensiero successivo.*



## Protezione fin dalla progettazione e protezione by default - Articolo 25 del GDPR

La privacy non dev'essere un pensiero successivo. L'Articolo 25 del GDPR definisce i concetti di protezione dei dati fin dalla progettazione e di protezione di default.

**Privacy fin dalla progettazione (Privacy by Design):** l'azienda deve proteggere la privacy lungo tutto il ciclo di vita delle operazioni, partendo dalla progettazione iniziale di sistemi e processi, fino al termine della vita utile dei servizi e alla cancellazione dei dati.

**Privacy per impostazione predefinita (Privacy by Default):** l'azienda deve garantire in maniera prestabilita che vengano raccolti ed elaborati solo i dati personali strettamente necessari. L'utente non deve aver bisogno di rifiutare di fornire ulteriori informazioni. L'azienda non può raccogliere maggiori informazioni solo perché ritiene di poterne avere bisogno in seguito.

## Tecnologie all'avanguardia: Articolo 32 del GDPR

L'Articolo 32 del GDPR sottolinea l'importanza di utilizzare le tecnologie più efficaci e aggiornate per supportare la governance delle informazioni:

*"Tenendo conto degli **avanzamenti tecnologici** ... il titolare e il responsabile del trattamento adotteranno misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio".*

Sebbene il GDPR non prescriva implementazioni tecniche specifiche, l'Articolo 32 indica come esempio, fra le altre, misure quali la cifratura, l'integrità, la disponibilità e i test per la valutazione di soluzioni tecnologicamente avanzate da parte dell'azienda.

## Creazione di una struttura EMM per il GDPR

Le soluzioni EMM, come MobileIron, sono una componente importante di un programma di sicurezza conforme al GDPR. Un'azienda che non utilizzi EMM con efficacia può trovare difficile giustificare alle autorità le motivazioni per cui non ha adottato misure tecniche avanzate per ridurre il rischio di perdita di dati.

*Un'azienda che non utilizzi EMM con efficacia può trovare difficile giustificare alle autorità le motivazioni per cui non ha adottato misure tecniche all'avanguardia.*

Un programma EMM per il GDPR deve includere le seguenti funzionalità di MobileIron:

1. La piattaforma MobileIron consente di **applicare la cifratura dei dati** direttamente sul dispositivo monitorando le impostazioni di cifratura del dispositivo e fornendo una cifratura secondaria per le app e i dati aziendali.

2. La piattaforma MobileIron consente all'azienda di **stabilire un confine netto tra i dati personali e aziendali** sul dispositivo, senza conferirle l'accesso al contenuto delle app o degli account e-mail personali. Ogni azienda deve anche valutare se l'accesso ad altri tipi di dati personali, quali l'inventario delle app o l'ubicazione del dispositivo, rientri in finalità operative o di sicurezza giustificabili. In tal caso, lo scopo deve essere esposto e comunicato con chiarezza, istituendo proattivamente le misure appropriate per la privacy by default e il consenso.

3. La piattaforma MobileIron consente di **applicare l'accesso attendibile ai servizi aziendali.** MobileIron Access fornisce all'azienda la visibilità dei dispositivi mobili e delle app che tentano di connettersi ai servizi di backend, bloccando gli accessi non autorizzati. MobileIron Sentry protegge il traffico dei dati e, se necessario, lo instrada attraverso ulteriori gateway per la sicurezza e l'ispezione.

4. La piattaforma MobileIron consente all'azienda di **utilizzare audit log** per stabilire quali azioni che hanno portato all'infrazione dei dati abbiano avuto luogo e quali contromisure successive siano state adottate. In alcune situazioni, il periodo di notifica obbligatorio previsto dal GDPR è di sole 72 ore e richiede quindi risposte rapide.

5. La piattaforma MobileIron consente all'azienda di **applicare controlli per la prevenzione della perdita dei dati (DLP, Data Loss Prevention).** Tali controlli consentono di cancellare remotamente (wipe) i dati riservati da un dispositivo andato perso e garantire che le app aziendali su un dispositivo non possano condividere dati con app non autorizzate. I controlli consentono inoltre di identificare gli attacchi all'integrità del sistema operativo del dispositivo mobile ai fini di verificare se sia stato soggetto a jailbreaking o rooting. In caso di problemi di conformità, l'azienda può utilizzare la piattaforma MobileIron per mettere in atto il rimedio più adatto, ad esempio la notifica, la quarantena o la cancellazione dei dati.

*I dispositivi mobili non gestiti non sono in grado di supportare una strategia di difesa approfondita.*

## Implementazione di EMM per il GDPR

Ogni azienda interessata dal GDPR deve valutare il proprio modello di configurazione e implementazione EMM esistente. In primo luogo, la valutazione deve identificare i gap in cui il sistema EMM non viene sfruttato appieno ai fini della conformità al GDPR. Secondariamente, costituisce le basi per la progettazione e l'implementazione di un programma di monitoraggio continuo della conformità e di rimedio.

Gli elementi riportati di seguito costituiscono un punto di partenza per l'implementazione di EMM nell'ambito di un programma di sicurezza conforme al GDPR:

1. Integrare nella gestione tutti i dispositivi mobili che hanno accesso ai dati aziendali. I dispositivi non gestiti non sono in grado di supportare una strategia di difesa approfondita e applicare un livello ragionevole di sicurezza dei dati in caso di perdita o compromissione del dispositivo.
2. Utilizzare profili di configurazione aggiornati. Applicare policy per la password, la cifratura, la sicurezza del dispositivo, la connettività e altre funzioni importanti per l'operatività aziendale.
3. Distribuire tutte le app aziendali come app gestite tramite un app store aziendale in modo che possano operare all'interno di una struttura di sicurezza controllata dall'azienda.
4. Applicare adeguate policy di prevenzione della perdita dei dati (DLP) per proteggere i dati delle app sul dispositivo.
5. Applicare l'accesso controllato per tutti i servizi aziendali. Bloccare l'accesso da parte di dispositivi, app e utenti non autorizzati, non gestiti o non conformi. Non consentire la memorizzazione di dati riservati su un dispositivo che esula dal controllo e dalla visibilità dell'azienda.
6. Stabilire policy relative alla privacy e alla sicurezza e comunicarle regolarmente e con chiarezza ai dipendenti.
7. Generare log di audit utilizzo e inventario adeguati a supportare il processo di risposta rapida alle infrazioni.

## Conclusione

Un'azienda non può offrire una sicurezza adeguata dei dati personali se non è in grado di dimostrare di avere implementato controlli e procedure EMM appropriati, atti ad assicurare che i dati necessari siano protetti da minacce esterne e dall'uso o dalla divulgazione non autorizzati. La piattaforma MobileIron offre una struttura robusta per soddisfare i requisiti di conformità ai principi di riduzione dei dati, integrità, riservatezza e responsabilità previsti dal GDPR.