How EMM Helps with GDPR Compliance

Reasonable, common-sense security standards are becoming law in many regions of the world. In Europe, the General Data Protection Regulation (GDPR), enacted in April 2016, will become fully applicable on May 25, 2018. GDPR will bring the European Union (EU) under one comprehensive and harmonised legal system for data protection and privacy. The monetary penalties and reputational damage of non-compliance with GDPR are substantial – the maximum fines are the greater of 20 million euros or 4% of the company's worldwide revenue.

GDPR applies to controllers and processors in the EU as well as controllers and processors outside the EU if they process the personal data of EU individuals. "Controller" is

MobileIron

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

"EMM becomes crucial for GDPR compliance."

IDC (February 2017)*

defined as the organisation that decides the purpose and means of processing the personal data. "Processor" is defined as the organisation that handles the processing on behalf of and under the instructions of the controller. For the purposes of this document, we assume the controller and processor are the same entity: the enterprise with employees or customers in the EU.

A comprehensive and well-structured Enterprise Mobility Management (EMM) program will be an important part of an enterprise's GDPR compliance initiative. This document provides a framework for enterprises to proactively assess their mobile privacy and security policies and enforcement models. This document does not provide legal guidance. Each enterprise must ensure that its EMM deployment maps appropriately to its internal legal and compliance frameworks.

The principles for processing personal data under GDPR are standards-based and consistent with emerging privacy frameworks in other regions.

GDPR principles

Every employer holds some personal data. The common-sense starting point to GDPR compliance is to hold the minimum amount of personal data necessary and to take reasonable precautions to mitigate the risks for individuals.

While Europe leads the world in its focus on data privacy, the principles for processing personal data under GDPR are standards-based and consistent with emerging privacy frameworks in other regions. These principles include:

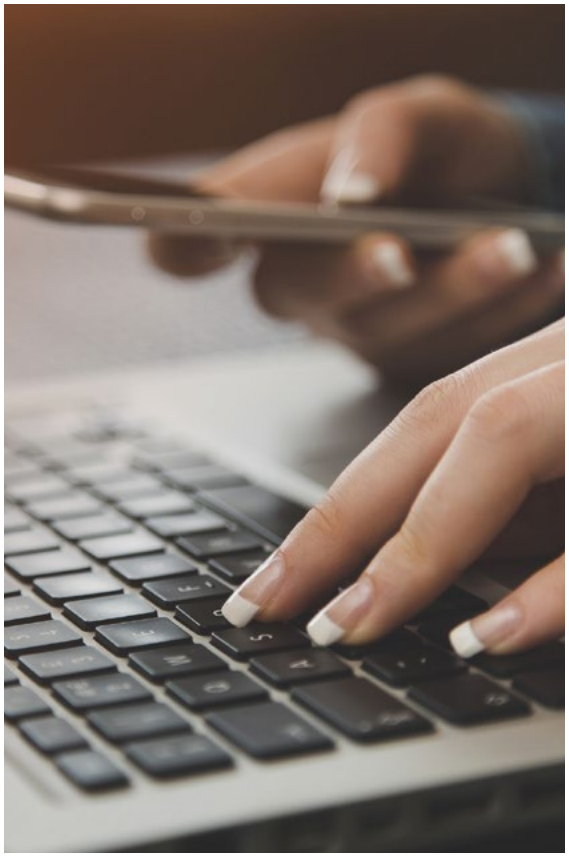
- **Lawful, fair, and transparent processing:** Enterprises must have valid grounds for processing personal data and must provide that information to individuals.
- **Purpose limitation:** There must be a clear and explicit reason for processing personal data. The data may only be processed for the purpose for which it was collected.
- **Consent:** The individual whose personal data is processed must generally provide consent.
- **Data minimisation:** The data processed should be limited to what is strictly needed for a specific purpose. Access should only be granted to those people who need it for that specific purpose.
- **Accuracy:** The data should be accurate, and inaccuracies should be easily rectified. Individuals should have the right to request such rectification.
- **Storage limitation:** The data should be retained for only as long as needed for the designated purpose.

* "Market Analysis Perspective: Western Europe Enterprise Mobility, 2017" by IDC Europe, February 2017.

- **Integrity and confidentiality:** The data should be processed in a manner that ensures appropriate security of the data, including protection against unauthorised processing and accidental loss.
- **Accountability:** The enterprise should be able to demonstrate compliance with and remediation for the above principles.

An enterprise needs to be able to show that it has adequate security in place and that compliance is appropriately monitored.

Privacy cannot be an afterthought.



Privacy by design and by default – Article 25 of GDPR

Privacy cannot be an afterthought. Article 25 of GDPR defines the concept of "data protection by design and by default," also known as "privacy by design and by default."

Privacy by design: The enterprise must protect privacy throughout the operations lifecycle, from initial process and systems design through service end-of-life and data deletion.

Privacy by default: The enterprise must ensure that, by default, only the needed amount of personal data is collected and processed. The user should not have to opt out from giving extra information. The enterprise cannot gather more information "just in case" it might want to use it later.

State of the art – Article 32 of GDPR

Article 32 of GDPR outlines the importance of using up-to-date, best-of-breed technologies to support information governance:

*"Taking into account the **state of the art** ... the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."*

Though GDPR does not prescribe specific technical implementations, Article 32 designates encryption, integrity, availability, and testing as sample measures, among others, for which the enterprise should evaluate state-of-the-art solutions.

Creating an EMM framework for GDPR

EMM solutions, such as MobileIron, are an important component of a GDPR-compliant security program. An enterprise that does not use EMM effectively may find it challenging to justify to authorities why it did not adopt state-of-the-art technical measures to mitigate the risk of data loss.

An enterprise that does not use EMM effectively may find it challenging to justify to authorities why it did not adopt state-of-the-art technical measures.

An EMM framework for GDPR should include the following MobileIron capabilities:

1. The MobileIron platform allows the enterprise to **enforce data encryption** on the device by monitoring encryption settings for the device and providing secondary encryption for business apps and data.
2. The MobileIron platform allows the enterprise to **establish a clear boundary between personal and business data** on the device. The enterprise does not have access to the content of personal apps or personal email accounts. Each enterprise must also assess whether access to other types of personal data, such as app inventory or device location, serves a justifiable security or operational purpose. If it does, then that purpose should be clearly articulated and communicated, and the appropriate privacy-by-default and consent measures proactively instituted.
3. The MobileIron platform allows the enterprise to **enforce trusted access to business services.** MobileIron Access gives the enterprise visibility into which mobile devices and apps are attempting to connect to back-end services. Unauthorised access can then be blocked. MobileIron Sentry protects the data traffic and can also route it through additional security and inspection gateways if required.
4. The MobileIron platform allows the enterprise to **use audit logs** to determine what actions took place leading up to a data breach and what, if any, subsequent actions were taken. In some situations, the mandatory notification period for GDPR is only 72 hours and requires quick response.
5. The MobileIron platform allows the enterprise **to enforce data loss prevention (DLP) controls.** These controls allow the enterprise to remotely wipe confidential data on a lost device and ensure that business apps on a device cannot share data with unauthorised apps. These controls also identify attacks on the integrity of the mobile operating system for jailbreaking or rooting the device. If there is a compliance issue, the enterprise can use the MobileIron platform to take the appropriate remediation action, such as notification, quarantine, or data wipe.

Unmanaged mobile devices cannot support a defense-in-depth strategy.

Deploying EMM for GDPR

Every enterprise impacted by GDPR should assess its existing EMM deployment and configuration model. First, this assessment will identify gaps where EMM is under-leveraged for helping with GDPR compliance. Second, it will form the foundation for designing and implementing an ongoing compliance monitoring and remediation program.

Here is a starting point for deploying EMM as part of a GDPR-compliant security program:

1. Place all mobile devices under management if they have access to business data. Unmanaged mobile devices cannot support a defense-in-depth strategy to enforce a reasonable level of data security on lost or compromised devices.
2. Apply up-to-date configuration profiles. Enforce policies for password, encryption, device security, connectivity, and other relevant business enablement functions.
3. Distribute all business apps as managed apps through an enterprise app store so that they can operate within an enterprise-controlled security framework.
4. Enforce appropriate data loss prevention (DLP) policies for the protection of app data on the device.
5. Enforce trusted access for all business services. Block access from unauthorised, unmanaged, or non-compliant devices, apps, and users. Do not allow confidential data to be stored on a device outside the visibility and control of the enterprise.
6. Establish and clearly communicate privacy and security policies to employees on a regular basis.
7. Collect appropriate inventory, usage, and audit logs to support a quick-response process for breach.

Conclusion

An enterprise cannot provide adequate security for personal data unless it can demonstrate that it has implemented appropriate EMM controls and procedures. These should ensure that the personal data required by the business is protected from external threats and unauthorised use or disclosure. The MobileIron platform provides a robust framework for compliance with the data minimisation, integrity and confidentiality, and accountability principles of GDPR.