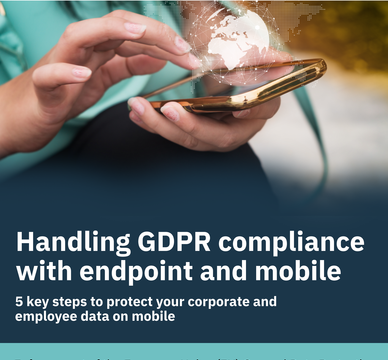

Handling GDPR compliance with endpoint and mobile

5 key steps to protect your corporate and employee data on mobile

Enforcement of the European Union (EU) General Data Protection Regulation (GDPR) applies to all global organisations processing personal data of EU data subjects. When it comes to your endpoint and mobile environment, are you confident that you can answer questions about:

- Where data is stored
- Whether it is stored securely
- Whether it is stored in compliance with ordinances and regulations
- Whether your corporate data is staying in-country
- How your end-user privacy is being protected

It's not just about your security: It affects your employees, partners and customers, too—choose wisely.

Data containment: Be sure your provider offers a secure container that helps ensure data is stored on the device, not on servers, preventing the providers' internal teams from viewing the data. In addition, make sure that personal data stored in the container is limited in scope to an as-needed basis, including name, address and phone numbers.

Data encryption: Look for the provider that uses AES-256 CTR encryption algorithms to encrypt all application (app) data in motion and at rest. For Apple iOS, look for built-in CommonCrypto FIPS 140-2-compliant encryption; for Google Android, look for SQLCipher with the OpenSSL (AES-256) FIPS 140-2-compliant crypto modules. This provides comprehensive encryption for databases—not just their contents.

Local presence: The intention behind GDPR requirements is to keep all the data your organisation touches secure. Seek the solution with contextually architected data centres that take regional ordinances into consideration. This will enable customers and their end users to expand the flexibility of their global mobile data transmissions.

Cognitive insights and analytics: Using augmented intelligence to see what happened, what can happen and what should be done—all with respect to your environment—can help you proactively address regulatory compliance needs. Having ample context related to your endpoint and mobile data can improve decision-making processes and can help IT and security leaders with their GDPR compliance.

Unified endpoint management (UEM): Picking a UEM solution with robust support for legacy and cutting-edge endpoint and mobile platforms can help maximise your alignment with GDPR requirements. Choosing a cloud-based platform that offers instant support for the latest operating system version updates will help you keep your bases covered.

Support regulatory mandates with an industry leader

IBM® MaaS360® with Watson™ cognitive UEM provides one window to manage and secure your mobile devices, laptops and desktops, including their users, apps, content and data. MaaS360 can support your GDPR compliance goals with features that include containment, cognitive insights and contextual analytics.

MaaS360 customers are protected, in the US, by legislation such as the Federal Information Security Management Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP)—in addition to ISO 27001, AICPA SOC 2 Type II, and FIPS 140-2 data encryption standards.

IBM MaaS360 | With Watson

Helping organisations meet their global data protection requirements

MaaS360 checks the box for major GDPR requirements related to endpoint and mobile—making it the optimal UEM partner to help your organisation prepare for compliance.

Capabilities and features	MaaS360
Container for locally storing information that limits personal data scope to as-needed data	✓
Management across mobile devices and laptops with UEM	✓
Contextual insights/analytics	✓
Comprehensive encryption of data at rest and in motion	✓
Ability to remove personal data on request	✓
Ability for data controllers to provide an electronic copy of the user's collected data upon request	✓
Availability of complete data maps to customers	✓
User consent prompted via acceptance of service agreements and end-user licence agreements	✓
Established processes addressing data subjects' access and rectification	✓
Established data breach response and notification protocols	✓
Privacy factored into products and procedures from the design stage onward	✓
Appointed data protection officer	✓
Audit capabilities and processes to support data protection authorities (DPA)	✓

IBM MaaS360 | With Watson

LEARN MORE. Find out how MaaS360 capabilities can support your goals for becoming GDPR-compliant.

Start a 30-day trial at no cost TODAY.

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey here.

55012755-USEN-00