ISEC7 EMM SUITE

WHITEPAPER - END USER DATA

Scope of the document

The following document provides an overview about the handling of end user data handling in the ISEC7 EMM Suite.

Introduction

The ISEC7 EMM Suite is a monitoring and management system for mobile infrastructure. The system is installed as a OnPrem solution at the customer site and so the customer is responsible for the processing and handling of collected end user data.

Is the ISEC7 EMM Suite GDPR compliant?

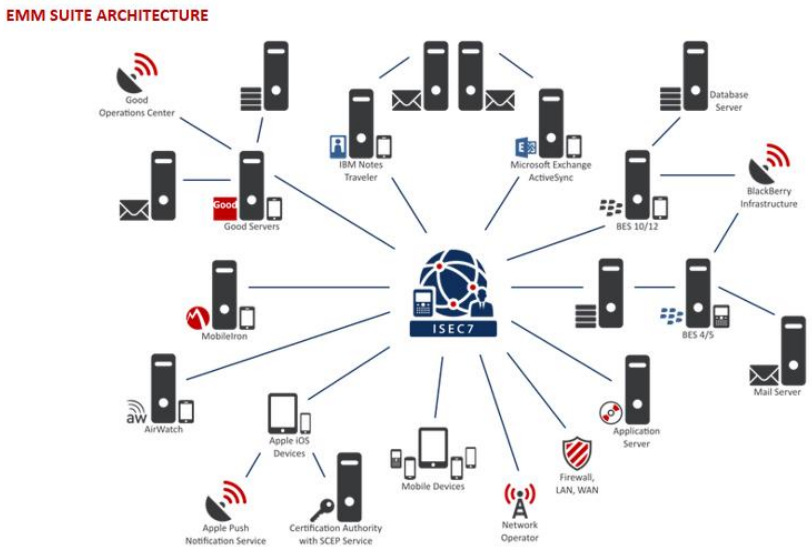
No, it can’t.

GDPR stands for General Data Protection Regulation and is the EC regulation in that field, which also has an extraterritorial effect, because it applies to every organization doing business with EU residents. Unfortunately, neither SaaS services nor software can be GDPR compliant.

GDPR is a regulation for organizations that regulates how to protect the individual’s PII (Personally Identifiable Information), which includes all data that could potentially be used to identify an individual. Thus, organizations must enforce GDPR compliance, which includes, e.g., implementing the new principles for user consent such as informed and unambiguous consent per purpose; the right to be forgotten; and many other requirements. GDPR also states that software which is used to handle PII must follow the principles of Security by Design (SbD) and Privacy by Design (PbD). Both are rather fuzzy principles, not being formally defined yet

ISEC7 EMM Suite data collection

Depending of the configuration the solution can monitor more than 750 parameters in a mobile infrastructure. The following architecture provides an overview about the interaction with corporate backend infrastructure and external system like network operators or NOC operators.



ISEC7 EMM Suite and end user data monitoring

The EMM Suite collects data from various systems in the mobile infrastructure and among many anonymous and infrastructure related data points, personal data of identifiable individuals is processed and stored. This includes:

- PIM related information
    - Log files of personal interactions with PIM systems, like:
        - Timestamp and activity type of synchronization for mail, calendar and contacts
        - Device ID was used by a user to access PIM data
    - Mailbox statistics
        - mailbox size
        - last access

- Network Operator & Location data
    - If location data is provided by the device / EMM system, it may be stored in the EMM Suite database for further utilization
    - If Carrier network ID and roaming ID is provided it is used to display information about logged in networks and allows an indirect information about the device / user location
    - if phone call and SMS information is provided by the device / EMM these data are used to provide compliance tracking for inbound and outbound communication from and to the device as well as content of the SMS. These settings are configured in the EMM system and can be limited to customers' requirements or data proception rules

- Personal information from corporate directories
    - User information can be gathered from corporate directories (e.g. Active Directory)
    - This can for example be used to search for users or devices and may include additional personal data like
        - telephone numbers
        - job position
        - department
        - others

- Application data
    - Information about the applications installed on devices
        - Application
        - Versions
    - Usage statistics of these applications are collected
        - Timestamp of access
        - Connection information (Successful connect or Error codes)

- HTTP traffic
    - Information of accessed URL is collected by the ISEC7 EMM Suite and analyzed to provide statistics and compliance information
    - This feature depends on the installed EMM system and may not be relevant for all ISEC7 EMM Suite customers

ISEC7 EMM Suite and end user data compliance

User related data is only stored, if it is available in the source system. If, for example, a user is deleted on the EMM or UEM server, the related information is removed from the EMM Suite as well. Statistics, loglines and other derived information that is stored in the EMM Suite is deleted after a configurable amount of days. Per default after 30 days, for both existing and deleted users.

Interaction of ISEC7 EMM Suite with vendor systems

Every instance of the ISEC7 EMM Suite is connected to ISEC7 licensing infrastructure to ensure proper licensing, update management and information about used EMM system version for development purposes only.

During a or connection to ISEC7's licensing infrastructure, the following data is transmitted to ISEC7 servers:

- ISEC7 EMM Suite information
  - Server identifier of the EMM Suite server sending the license request
  - Installed version of EMM Suite
  - Installed version of Tomcat
  - Java Runtime Environment information
  - Number of ISEC7 EMM Suite agents per Java runtime version
  - Version used by monitor and tomcat

- Number of users
  - Unique count of known mail addresses
  - User count per connected MDM / EMM type (e.g. BlackBerry, MobileIron...)
  - No transfer of personal data

- Number of devices
  - Unique count of device identifier
  - Device count per device type
  - No transfer of personal data

Data in Transport & Data in Rest

To protect end user data information while in transport the communication between the ISEC7 EMM Suite and related systems should be SSL encrypted.

All information gathered by the ISEC7 EMM Suite are stored in a Microsoft SQL database. To protect end user data the SQL server can be configured with SQL encryption.