Datasheet

Protection and control for mobile end devices

IKARUS mobile.management resolves the complex demands on the flexible use of mobile end devices in corporate environments. The software, which is TÜV-verified, tested in independent audits, developed exclusively in Europe and hosted in Austria, meets all the guidelines of European data protection as well as all requirements of a modern and flexible working environment.

IKARUS mobile.management is a highly professional complete solution with mobile device management (MDM), mobile application management (MAM), mobile content management (MCM) and mobile security management (MSM). The particularly flexible cloud service manages and protects smart phones, tablets and notebooks against threats through malware, loss of data and unauthorized access to data and systems.

Flexible work, independent of location and end devices

The digitization and networking of our channels of communication not only bring advantages. They also open up new attractive points of attack – particularly in the corporate environment, where company secrets as well as personal data are concerned. Employees' mobility and productivity are supported through the use of laptops and smart phones. At the same time, data security, compliance with corporate policies and legal frameworks must be guaranteed. The balancing act between strict provisions and flexible use requires an intelligent solution.

Meet data protection obligations and gain control

All companies that work with EU citizens' data must demonstrably prove that suitable state-of-the-art organizational and technical security provisions are also adhered to for mobile end devices. Laptops, smart phones and tablets must therefore be encrypted and backups generated. Additional gateways, for example through authorisations for apps installed on the devices, must be secured. Hence, only certified apps may be installed and in case of doubt, it must be feasible to delete all company data remotely. Private data and apps must be kept separate from corporate data, for example by using container solutions. This is the only way to completely and verifiably prohibit unauthorized data access and disclosure.

At the same time, the containers can secure the encryption of the corporate data and communication between the mobile end device and the IT department. Furthermore, all risks and security measures must be reviewed, evaluated and documented on a regular basis.

A suitable mobile management system offers a detailed overview of all devices with access to corporate resources at a glance. Devices and applications can be managed centrally and inventoried. The software distribution, including the rollout of updates and licences should be managed centrally of course including efficient malware protection, remote control features and automated action in case of security breaches.

Comprehensive protection, central overview, simple management

IKARUS mobile.management provides you with an overview and control over the mobile access your users have to corporate resources. Individual access rights and remote configuration and management of the mobile devices allow your company policies to be implemented reliably across all systems. They protect devices and data against unplanned and unauthorized access, and loss of data, knowledge and company secrets. Using a central, customizable dashboard, flexible policies can be defined and the status of the systems and devices monitored. If company provisions or security guidelines are breached, predefined actions can be performed automatically.

IKARUS mobile.management allows simple and quick tailored solutions to be created for the efficient management of your mobile devices, applications and data. The cloud service is equally suitable for small companies and for enterprises – any amount of end devices can be connected. Invoicing is dependent on the number of licences. The benefit of security: All data is processed only in servers located in Austria in the ISO-certified A1 data center in Vienna (Security Compliance according to ISO 27001 Managing Information Security, ISO 27018 Protecting Personal Data and CSA Star Securing Cloud Computing Environments). The Austrian and EU data protection laws apply in full.

Mobile solutions will also play a key role in future in our private and working life. It is therefore appropriate to invest in a future-proof solution: Professional concepts, simple to operate and reliable methods are worthwhile. Those who neglect their data protection obligations must expect to pay high penalties.

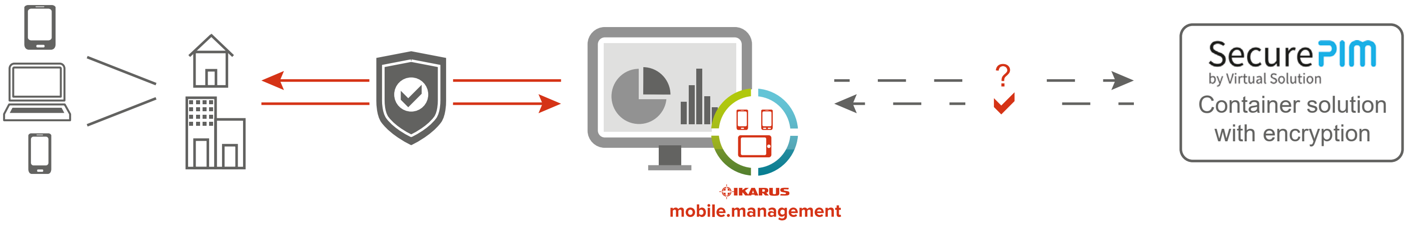

Figure 1 - Central mobile management system for secure and controlled use of mobile devices in corporate environments

Advantages

- Full coverage of all leading platforms (Android, Android for Work, Samsung KNOX, iOS, Windows 10, Windows 8 Phone, Symbian) through a single user interface
- TÜV certification – unique in Europe since the introduction of EU GDPR
- Data processing is carried out exclusively in the IKARUS data-processing centre in Vienna
- Highest possible data security and data protection under EU GDPR
- BYOD-compatible: Separation of business and private data

Features

- Mobile device management (MDM with asset management, integration in the central user-administration, configuration through automated rules and remote access as well as monitoring via a web-interface and configurable reports.
- Mobile application management (MAM) with app security with database access to security-relevant app evaluations android mobile security to protect against malware from apps and internet, container support for password protection and separation of business and private data as well as one’s own enterprise app store.
- Mobile content management (MCM) with secure access gateway for flexible management of the access options to corporate resources incl. firewall, data access per VPN for dedicated apps, GDPR-compliant BYOD management and self-service portal
- Mobile security management (MSM) with protection against unauthorized access, security management, virus and malware scanner for android, rollout and management of templates and guidelines, monitoring the settings and policies, automated actions in case of compliance breaches.

»Mobile solutions play a leading role in our private and working life, now and further in the future. It is therefore appropriate to invest in a future-proof solution: Professional concepts, simple to operate and reliable methods are worthwhile.«

Christian Fritz - COO, IKARUS Security Software

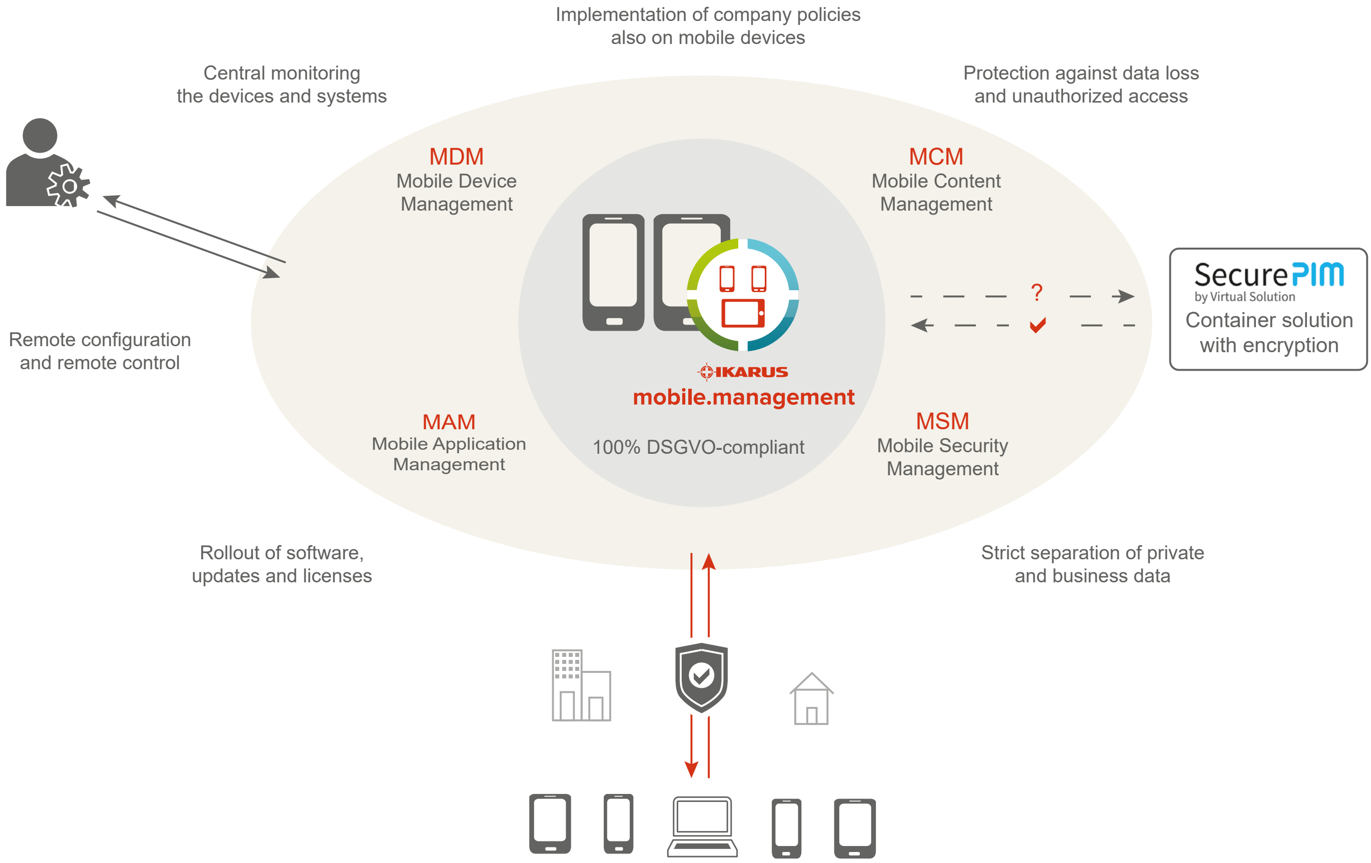
Implementation of company policies also on mobile devices
Central monitoring the devices and systems
Protection against data loss and unauthorized access
MDM
Mobile Device Management
MCM
Mobile Content Management
SecurePIM
by Virtual Solution
Container solution with encryption
?
Remote configuration and remote control
IKARUS
mobile.management
MAM
Mobile Application Management
100% DSGVO-compliant
MSM
Mobile Security Management
Rollout of software, updates and licenses
Strict separation of private and business data

Figure 2 - **IKARUS mobile.management** enables the central administration, security and control of mobile devices and meets all requirements of the EU GDPR.

IKARUS mobile.management: TÜV Trusted App

The MDM solution **IKARUS mobile.management** is a result of a development partnership between **SEVEN PRINCIPLES AG** and **IKARUS Security Software GmbH.**

7P is the leading German manufacturer of enterprise mobility solutions for the secure management of smartphones and tablets.

IKARUS is the leading Austrian provider of IT/OT security solutions and develops trend-setting security technologies based on the IKARUS scan.engine.

Together, with **IKARUS mobile.management** we offer you a complete solution to optimize and secure your mobile communication and work processes. DSGVO compliance and TÜV certification included.

TÜV
TRUST IT
TRUSTED APP
TÜV AUSTRIA Group

- ✓ Certified privacy
- ✓ Certified information security
- ✓ Certified security measures

GDPR-Compliance: Security and Data Protection To-Go

The digitalisation and integration of our communication channels does not only benefit our working life, it also provides attackers with an attractive new target. Therefore, the EU GDPR, which entered into force in 2018, placed certain demands when processing personal data of EU citizens (see Article 5, **„Principles relating to personal data processing“**):

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality

> *According to Article 5 (2), the controller shall be responsible for, and be able to demonstrate compliance with these principles (“**Accountability**”).*

IT departments are facing new challenges. According to Article 32 (“Security of processing”), companies have to ensure demonstrably that their mobile devices follow all security guidelines:

- the pseudonymization and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to per sonal data in a timely manner in the event of a physical or technical incidentn
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Therefore, laptops, smartphones and tablets need to be password-protected, data has to be encrypted and backups are required. Additional backdoors like app permissions need to be protected by prohibiting the download of unwanted apps without permission and by optionally deleting all company data via remote control. Only certified apps may be installed and in doubt, all company data needs to be deleted via remote control. All private data and private apps need to be strictly separated from company data – for example by containerizing. This is the only way to completely and demonstrably prevent unauthorized access and unauthorized disclosure. At the same time, the containers ensure the encryption of all company data and of the communication between the mobile devices and IT departments.

All risks and security measures need to be assessed and documented (see Article 35, “Data protection impact assessment”). Article 32 (1d) also demands “a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing“. Without MDM, the compliance with all rules according to the state of technology is hardly possible.

Mobile devices: Flexible usage despite of strict guidelines

A suitable MDM system offers a detailed overview of all devices that may access company resources. Devices and applications can be centrally managed and inventoried. Software distribution, updates, and licences should be managed centrally – of course including powerful malware protection and the possibility to prevent unauthorized access and start automatic actions in case of security breaches.

Mobile solutions will be playing a major role in our future business and private life. Therefore, we recommend choosing a sustainable solution: Professional concepts, easy handling and reliably solutions will be worth it. Not least because of the severe penalties in case of non-compliance: Neglecting the data protection obligations shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83 (5), “General conditions for imposing administrative fines”).

Questions?

We will be happy to advice you! Contact us at sales@ikarus.at or Tel. +43 1 58995-500. Or visit our website at www.IKARUSsecurity.com/ikarus-mobilemanagement.