# SecureContainer - DME

## Make your mobile workspace ready for GDPR with a single app

The General Data Protection Regulation becomes effective **May 25, 2018**. With its enforcement date approaching Data Leakage Prevention (DLP) has risen to the top of security initiatives organizations are looking to implement. While the GDPR is not prescriptive in terms of what technologies are required for compliance, here are some key points to consider in making your mobile workspace ready for GDPR.

### Stop human errors

Keep your data safe and prevent it being used in personal applications.

- DME prevents users from copying or sharing sensitive data
- DME has certificate based device authentication and Single-Sign-On using AD, LDAP
- All data is encrypted in the container to keep your data safe when leaving the container

### Manage lost / stolen devices

Prevent company data being copied on lost or stolen devices.

- The IT-administrator can manage the DME of business owned devices and BYOD; lock and wipe the secure container remotely.
- The enforcement of password controls can be done by the IT-administrator
- The IT-administrator can manage the MDM settings and provide users tools to do a remote wipe, lock the device and clear the password.

### Prevent blind spots

Know what data and how users are accessing the data on their mobile devices.

- The management console provides total visibility and full control of mobile devices
- Enforce separate policies for different user groups, BYOD and corporate owned devices
- Ensure users can only store, view and edit files within the secure container

### Malware attacks

Secure your company data on mobile devices from becoming an entry vector for malware.

- DME detects rooted or jailbroken devices
- DME protects corporate data in the secure container from malware on the device
- DME enables remote wiping of the DME app or full device

### Prevent data leakage

Prevent data leakage between applications by separating business from personal information.

- DME fully separates personal data from business data
- DME keeps all business apps and data stored in the encrypted container at all times

### Microsoft 0365 data security

Increase DLP security and prevent leakage of login and password information.

- Add an extra layer of security with Single Sign On (SSO) login using AD password, unlock pattern or touch ID
- Add more security with the single app container provided with DME
- Configure the DME app with policies and certificates allowing users to access email, PIM, intranet, file shares and other web applications

Soliton SecureContainer - DME 5.0 provides secure access to your company data via smartphones and tablets, prevents sensitive business data from being copied. The business data is encrypted and stored in the secure container.


**EMEA office**
Soliton Systems Europe N.V.

Gustav Mahlerplein 2
1082 MA Amsterdam
The Netherlands

+ 31 20 301 2166
emea@solitonsystems.com
www.solitonsystems.com


Soliton®