baramundi

Fact Sheet

Unified endpoint management (UEM) as a building block for GDPR compliance

As of May 2018, companies have to comply with the requirements of the new EU GDPR (European General Data Protection Regulation). Collecting, forwarding and storing personal data in compliance with data protection laws presents companies with various new challenges. As a result, internal procedures have to be established (e.g. procedure directories), evaluated (e.g. risk analysis), documented, and regularly updated. Technical and organizational measures (TOMs) have to be developed, and GDPR principles have to be implemented in companies' IT infrastructures.

A comprehensive UEM system is an important part of the initiative to meet or achieve GDPR compliance for any company. However, compliance is usually a comprehensive process that needs to consider various components, such as technology, policies, and organizational issues. The baramundi Management Suite (bMS) is a UEM system that addresses many use cases related to the GDPR principles. The following explanations illustrate the solutions bMS offers for the stationary and mobile infrastructure of a company.

	GDPR principles	Use case in the company	bMS solution
GDPR compliance	Compliance of operating systems	In the company, **Windows 10** is to be rolled out to all coworker PCs. However, IT managers want to define **privacy-compliant** **settings** for the upgrade beforehand.	**baramundi OS Install** supports the installation and configuration of **Windows 10**. It can be configured with company-specific data privacy requirements (e.g. deactivating Cortana, not sending usage statistics) – provided these are supported by the respective Windows editions.
	Compliance of mobile apps	The company has strict privacy policies and, therefore, all employees may only run **GDPR-compliant apps** on their mobile devices.	By means of mobile application management, administrators determine which applications employees can use. This works via the **baramundi app black and white listing**. The lists thus offer protection against potentially dangerous or unwanted apps, such as applications that demand too much data access.
	Compliance of app-specific settings	Some of the apps that employees have on their smartphones are very data-hungry, and the specific usage purpose for the personal information they collect is sometimes questionable. However, due to acceptance or usability, these apps cannot be completely banned within the company. Therefore, the administrator must take the opportunity to configure such apps securely and in compliance with data protection regulations.	The ability to pre-configure app settings helps ensure that the data is used correctly. **baramundi Mobile Devices** enables the distribution and configuration of apps (for example, via secure HTTPS communication) by using native means of operating system vendors with **AppConfig** standard mechanisms.
	Protecting personal data on mobile devices	On their mobile devices, employees also use personal information (such as contacts, appointments, private notes and e-mails) that has to be strictly isolated from the other company data.	One option is to use a **container solution**. With baramundi Mobile Devices, the simple and intuitive configuration of a container solution is possible. Another possibility is to use the **native options of Android and iOS** to keep data separate. The configuration of these options is supported in bMS version 2019 R2.
Requirements	Art. 32, para. 1a GDPR: Encryption of personal data	Unintentional disclosure of sensitive business information and the loss or theft of mobile devices such as laptops, tablets, and smartphones can cost a business millions in damages. IT managers wish to minimize this risk.	With the help of **baramundi file and disk protection powered by DriveLock**, it is possible to encrypt hard disks, mobile devices (e.g. memory sticks) or even specific files according to certified procedures. As a result, sensitive information can be reliably protected against access by unauthorized third parties. The Windows operating system feature, **BitLocker** drive encryption, is also supported in bMS.
	Art. 32, para. 1d GDPR: Regularly testing the effectiveness of security measures	IT managers in a company wish to secure their own IT infrastructure in accordance with GDPR, highlight **weak points**, minimize risks, and prioritize measures.	**baramundi Vulnerability Scanner** helps in regularly checking the effectiveness of security measures. It regularly scans the IT infrastructure for vulnerabilities, initiates processes for their elimination (e.g. patches or software updates with **baramundi Patch Management**) and shows whether they have been successful.

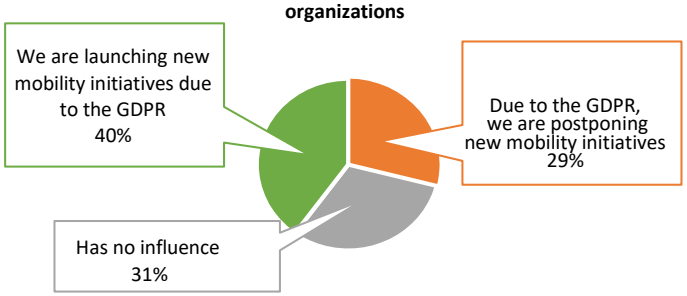
	GDPR principles	UseCase in the company	bMS solution
Requirements	Art. 15 GDPR: Right of access by the data subject	An employee in the company wishes to know from his administrator what personal data concerning him has been stored.	The personal data used in the bMS (e.g. IP addresses) can be viewed and exported by the administrator as needed.
	Art. 25 GDPR: Data protection by design/default	An employee does not wish **energy data or application usage data** of his computer to be captured.	By default, the collection of energy data (**baramundi Energy Management**) or application usage data (**baramundi AUT**) is disabled for each client in the bMS and can be manually enabled if required.
	Art. 17 GDPR: Right to erasure ('right to be forgotten')	An employee leaves the company and wants his personal data to be **deleted**.	In the bMS, the administrator has thea option of displaying the stored personal data and deleting it.
General	Art. 5 GDPR: Accuracy	The IT administrator relies on the fact that all infrastructure data is **up to date** in order to take the **right** measures to manage the infrastructure.	With **baramundi Inventory** and **baramundi Network Devices**, the entire IT infrastructure can be inventoried to show a constantly updated "image" of the hardware and software.
	Art. 5 GDPR: Confidentiality and integrity	In order to be able to correct an error, it is sometimes necessary for customer **databases** or parts of them to be sent to baramundi anonymously.	baramundi supports error analysis with anonymized data. Using **baramundi DBAnonymizer** it is possible to **anonymize** the customer's databases and then use them for the analysis.
	Art. 5 GDPR: Limitation to specific purposes	The IT managers in the company have to know what personal data is processed in the software products they use.	In general, the **purpose limitation** of the collected data is provided in the accompanying documentation of the software. The personal data processed in the bMS is described in the **manual** for each module and its purpose is documented.

More information: baramundi.com/GDPR

GDPR as an opportunity

The use of mobile technologies in companies is irreversible. As a result of the GDPR, most companies tend to see the need to perform new mobility initiatives in order to improve the security and compliance of company data on mobile devices. In addition, the GDPR offers a binding framework and, therefore, legal certainty for the handling of personal data, which in turn motivates investment.

Consequences of the EU GDPR on mobility initiatives within organizations



Without an efficient UEM solution, it will be difficult for companies to implement the GDPR IT security requirements throughout their IT infrastructure.

bMS privacy compliance

GDPR compliant

"For years the bMS has taken account of the provisions of the German Data Privacy Act and as such makes an important contribution to customers' data protection compliance. Version 2018 R1 of the bMS also takes into account the principles of the EU GDPR."

Dr. Lars Lippert, CEO baramundi software