baramundi

Fact Sheet

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

As of May 25, 2018, companies have to comply with the requirements of the new EU GDPR (European General Data Protection Regulation). Collecting, forwarding and storing personal data presents companies with new challenges for the future. As a result, internal procedures have to be established (e.g. procedure directories), evaluated (e.g. risk analysis), and documented. 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	UseCase 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. Prior to this, IT managers wish to define **privacy-compliant settings** for the upgrade, though.	**baramundi OS Install** supports the installation and configuration of **Windows 10 in-place upgrades**. These upgrades can be configured with company-specific privacy requirements (such as disabling Cortana, not sending usage statistics).
	Compliance of mobile apps	The company has strict privacy policies and, therefore, all employees may only have **GDPR-compliant apps** on their mobile COPE (corporate-owned, personally-enabled) 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 provide protection against potentially dangerous or unwanted apps, such as those that require overly comprehensive data access.
	Compliance of app-specific settings	Some of the apps that employees have on their smartphones are very data-hungry, and limiting the purpose of the personal information they use is sometimes questionable. Due to acceptance or usability, though, these apps cannot be completely forbidden by the company. Therefore, the admin has to take the opportunity to configure such apps in compliance with data protection.	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, notes and e-mails) that has to be strictly isolated from the other data.	In this context, a **container solution** offers a clear separation between private and business data on the device. With baramundi Mobile Devices, the simple and intuitive configuration of a container solution (such as SecurePIM by Virtual Solution AG) is possible. The encryption of the SecurePIM container is so effective that it ensures a "reasonable level of protection" within the meaning of Art. 32 GDPR for personal data.
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**, it is possible to encrypt hard disks, mobile devices (e.g. memory sticks) or even specific files according to certified procedures (FIPS 140-2). As a result, sensitive information can be reliably protected against access by unauthorized third parties.
	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 compliance management** helps in regularly checking the effectiveness of security measures. It regularly scans the IT infrastructure for vulnerabilities, initiates processes for their elimination (e.g. patching [**baramundi patch management**] or software updates [**baramundi managed software**]) and shows whether they have been successful.

baramundi

	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 wishes his personal data to be **deleted**.	In the bMC, the administrator has the 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	As a result of worldwide **cyberattacks** (e.g., WannaCry), the admins wish to be sure that the data in the utilized UEM solution is not accessible to third parties and cannot be falsified.	Through internal procedures that are documented and performed by a **security expert team**, baramundi ensures that potentially critical security vulnerabilities in the bMS are quickly found, fixed and made available to all customers. This ensures that the system itself is also protected against attackers.
	Art. 5 GDPR: Purpose limitation	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.

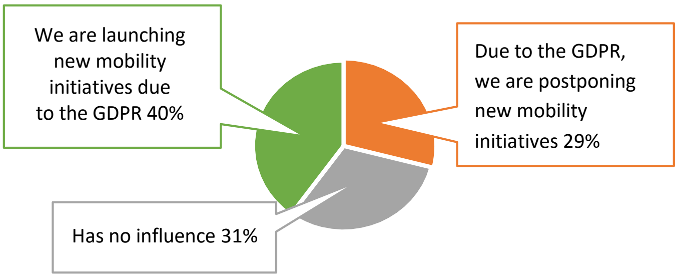
More information: baramundi.com/GDPR

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 DSGVO IT security requirements throughout their IT infrastructure.

Source: IDC Multi-client study, August 2017

bMS privacy compliance

"For years, the bMS has been taking account of the provisions of the Federal Data Protection Act (BDSG), thereby making an important contribution to customer privacy. Version 2018 R1 of the bMS also takes into account the principles of the EU GDPR."

Dr. Lars Lippert, CEO baramundi software