White Paper

GDPR is now only one year away - how data security prepared are you?

Executive Summary

Now that the EU General Data Protection Regulation (GDPR) has been passed, EU residents will soon have a consistent level of protection and a better say in how their data is handled. On the other side, businesses in the EU and international corporations doing business with the EU will soon be legally obliged to protect personal data throughout its lifecycle. Non-compliance with the new regulation can result in massive fines, as high as €20 million or 4% of a company's global annual turnover. However, there are some real opportunities for European businesses due to the new regulation. First and foremost: Harmonization. Currently, there are 28 different data protection schemes for businesses to understand. GDPR will harmonize data protection regulations across the EU, superseding existing national data protection laws that each member country has in place. Although the standards will be far more stringent for most EU countries, and will require the implementation of many new data protection measures, this consistency should simplify doing business within the EU.

With the deadline only 12 months away, the key questions every business should be asking at this point are:

Does the GDPR apply to my organization, i.e. do we process data of EU residents?

What data format do our personal data sets have and where is that data stored?

Are we using suitable technology to protect sensitive data?

What security strategy should businesses employ to avoid fines?

There is a silver lining for companies tackling the upcoming challenges: State- of-the-art security technology, which assists companies in becoming compliant and help lessen the impact of the regulation, is available today and should be an integral part of any corporate data protection strategy. While the GDPR is not a legislation about data protection and cyber security, compliance to the regulation requires the latest cyber security technology in order to implement suitable concepts. Such security technologies include encryption, access control and strong authentication solutions.

In order to reduce the impact of the new regulation, it is essential for businesses to develop an overall security concept that takes a holistic approach to data management. This includes the collection, processing, retaining and managing of sensitive data. The GDPR specifically mentions encryption and pseudonymization as appropriate safeguards for securing data. Both approaches follow the principle of data protection by design, ensuring privacy protection throughout the data lifecycle. Encryption can be used to avoid the need for breach notification, which the regulation expects to take place within 72 hours after the discovery of data breach, as it renders the private data unintelligible.

What is the General Data Protection Regulation (GDPR) and how does it affect international business?

At the core of the new regulation is the governance of information that relates to individuals across the EU member states. It is an overdue legislative response to the increase of data breaches and the huge financial burden that these attacks result in for businesses across all sectors internationally. It will replace the 1995 Data Protection Directive 95/46/EC, which, due to margins of interpretations within member states when implementing national laws, became an ineffective patchwork of different privacy laws. Additionally, the speed of technological change regarding data storage and dissemination, the advent of disruptive technologies, a steady increase in security breaches and the rapid onset of globalization, meant that a new regulation was deemed necessary.

The new EU GDPR, which comes into effect on May 25th 2018, defines minimum standards for handling, securing and sharing personal data of EU inhabitants. It applies to businesses based in the EU as well as all organizations outside the EU who are processing personal data of EU residents. Unlike the 1995 directive, the GDPR is directly applicable to each member state and does not need to be translated into national laws before coming into effect.

The regulation affects the complete lifecycle of data management. Very importantly, the definition of personal data is now broader:

“Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

Obtaining consent for processing personal data under the GDPR must be clear and must seek affirmative response. When it comes to personal data of children under the age of 16, parental consent is required before processing is permitted.

Security objectives of the GDPR

There are a number of key security objectives that GDPR is being put in place to tackle;

- Establish data privacy as a fundamental right. The GDPR considers data protection a fundamental human right of an individual, which includes a "right to the protection" of their personal data. Anyone based in the EU, or anyone handling or targeting the personal data of an EU-based individual must have processes, technology, and automation to effectively protect personal data.
- Clarify the responsibilities for EU data protection. The GDPR applies to a controller or a processor who is based or established in the EU, or to a company not based in the EU but who offers goods or services from outside the EU borders to a data subject in the EU or who monitors the behavior of data subjects in the EU.
- Define a baseline for data protection. To avoid fragmentation and ambiguity, GDPR has set a baseline for data protection by requiring anyone processing the personal data of an individual that is in the European Union to follow the requirements laid down in the GDPR.
- Elaborate on the data protection principles. The GDPR considers encryption as one of the components of a broad security strategy, and mandates that organizations need to consider assessment, preventive, and detective controls based upon the sensitivity of the personal data they have.
- Increase enforcement powers. The EU aims to ensure compliance with the GDPR by enforcing huge fines of up to 4% of the global annual revenue upon non-compliance.

Under the current law, as contained in the Data Protection Act (DPA), the same rules apply, regardless of the size of an organization. However, the General Data Protection Regulation (GDPR), which will replace the DPA, recognizes that SMEs require different treatment from both large and public enterprises.

GDPR includes new obligations and liabilities for businesses, specifically:

- Provision of an appropriate level of security
- Data breach notifications to controllers
- A dedicated Data Protection Officer
- Complete record-keeping that that can be produced upon request
- Direct liability to pay compensation
- Policing of controllers and assistance with the controller's compliance with its security obligations
- Reporting of incidents within 72 hours and presentation of relevant logs within 72 hours
- Proper impact assessments and prior consultations with data protection authorities
- Clear explicit consent required from the person concerned to process their personal data. The business collecting the data must clearly express how it intends to use the data it collects or with which it has been entrusted.

- The right to be forgotten on request. This newly established right forces businesses to provide “the clear and straightforward possibility” of erasing an individual’s or another business’s data simply upon request.
- The right to move data from one service provider to another. The business will take responsibility for this procedure that must be easy, quick and upon the contact’s request.

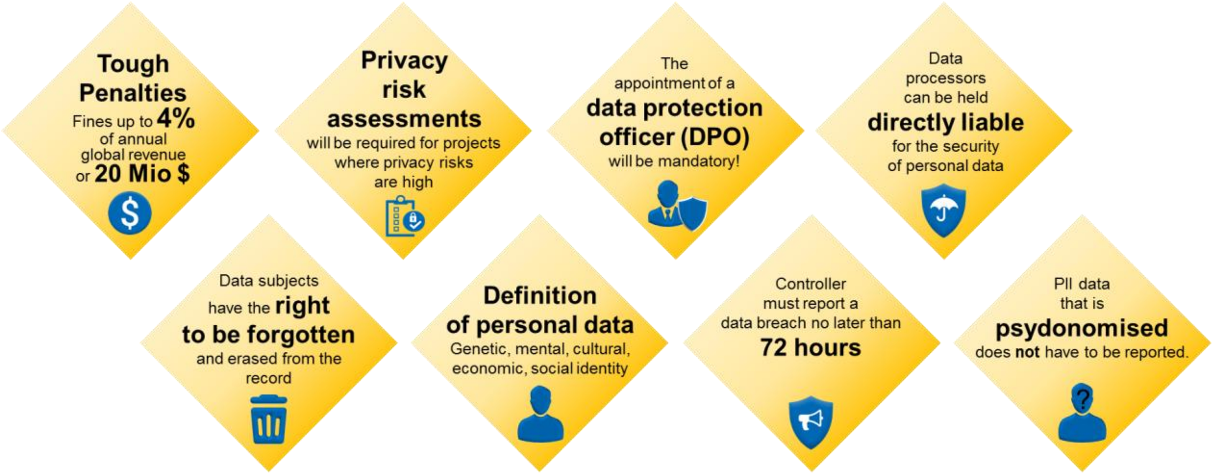

Tough Penalties
Fines up to 4% of annual global revenue or 20 Mio $
Privacy risk assessments
will be required for projects where privacy risks are high
The appointment of a data protection officer (DPO) will be mandatory!
Data processors can be held directly liable for the security of personal data
Data subjects have the right to be forgotten and erased from the record
Definition of personal data
Genetic, mental, cultural, economic, social identity
Controller must report a data breach no later than 72 hours
PII data that is psydonomised does not have to be reported.

Figure 1: Main attention points of GDPR

Failure to conform to these obligations can now result in fines of up to 4% of global annual turnover, or €20 million, for serious violations.

What sets the GDPR apart from earlier legislation, relating to the protection of private data, is the paperless, digital and transitional aspects of the data from a legal viewpoint. This gives rise to a host of critical issues in cybersecurity and also marks the first time that data is being considered in a borderless context.

GDPR impact beyond Europe

Beyond Europe, for US multinationals the burden to ensure compliance with the new incoming GDPR is pretty steep, but one that US multinationals are facing up to. Ninety-two percent of U.S. multinational companies cited compliance with the looming General Data Protection Regulation (GDPR) as a top data protection priority, according to new research from PwC. Sixty-eight percent are earmarking between $1 million and $10 million on GDPR readiness and compliance efforts, with 9% expecting to spend over $10 million.

US corporations that are heavily invested in Europe will probably stay the course in the near term. Indeed, 64% of executives reported that their top strategy for reducing GDPR exposure is centralization of data centers in Europe. Just over half (54%) said they plan to de-identify European personal data to reduce exposure and impact of the regulation. The threats of high fines and impactful injunctions, however, clearly have many others reconsidering the importance of the European market. In fact, 32% of respondents plan to reduce their presence in Europe, while 26% intend to exit the EU market altogether.

Terminology and roles within GDPR

To understand the various roles that relate to GDPR implementation and how they relate to one another, here is a hypothetical manufacturing company called MAGNET, who for this example, is based in Belgium. Customers of MAGNET are placing their online orders through the company's web site.

As part of its multi-national business model, MAGNET stores and processes the personal information about individuals ("Data Subjects").

MAGNET, as an EU-based company, determines the purposes and the means of the processing of personal data ("Controller").

The development, testing, customer care & billing efforts are outsourced to external subcontractors in China and Thailand ("Processors") where the employees often copy their customer's data ("Personal Data") to their local systems for development, testing, and processing, respectively.

MAGNET also partners with payment and delivery companies ("Third parties") of different countries and provides them with individual's data ("Personal Data") for the processing of an order.

An independent public authority monitors the application of the GDPR ("Supervisory Authority").

Businesses using a cloud environment must pay special attention to GDPR

Ever since the EU GDPR was voted in, businesses have started their countdown to the transition. With twelve months to comply with the new European regulation and the consequences of its requirements in terms of data protection: strengthened cyber security, liability of data collection entities and new mandatory procedures.

According to Ovum, 70 per cent of businesses expect to increase spending to address data protection and sovereignty. A major driver for this is that failure to do so after the two-year transition period will mean businesses face significant consequences, including regular data protection audits.

Millions of businesses are currently migrating their data into the cloud, which will account for why Gartner projected public cloud services growing 17.2 per cent in 2016. And it is this vast expansion that means the issue of protecting European data now has a whole new dimension.

For many organizations, the cloud will be seen as an especially glaring gap in their data protection strategies. As dependency on cloud applications grows, enterprises face a growing number of issues regarding data privacy, compliance and security. With cloud, user data is more exposed compared to when it was solely confined to local systems, increasing the risk for potential GDPR violations in the event of a data breach.

Controllers and processors must take security measures appropriate to the processing of data and its risks (GDPR Articles 26(2)(c), (f), (h), 30). A controller knows the nature/purposes of its intended processing and can secure its data by encrypting data pre-upload or implementing backups internally or to another cloud, for example.

Safeguarding Personally Identifiable Information (PII): Encryption vs. Pseudonymization

Encryption and pseudonymization are both considered within the GDPR as security protection measures (see Article 32) and successful implementations will ensure that companies can avoid heavy financial penalties in case of a data breach.

With pseudonymization, the GDPR introduces a new concept into European Data Protection Law as a means of protecting the rights of individuals. Data that has been pseudonomized is not exempt from the GDPR, however, provisions are greatly relaxed for controllers using this kind of personal data. Pseudonymization can be described as a process, which neither renders data anonymous, nor does it allow identification. It stands for the separation of data from direct identifiers, so that data cannot be linked to an identity without additional information that is held separately.

The GDPR encourages pseudonymization, but the separation of personal data from data sets is a process many corporations will find difficult to implement, as it requires a complete assessment of existing data resources and the creation of a data map. In this case, the GDPR recommends encryption as a security measure, e.g. Article 32, Security of Personal Data, states that the "controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including… encryption of personal data." Under GDPR, appropriate encryption has the specific benefit of removing the requirement to notify data subjects (individuals) in the event of a data breach.

In order to comply with the new regulations, corporations will need to implement different encryption methods within their infrastructures, such as

- Servers, including file, application, database, and full disk virtual machine encryption.
- Storage, including network-attached storage and storage area network encryption.
- Media, through disk encryption.
- Networks, for example through high-speed network encryption.

Also, strong key management is required to protect the encrypted data and to ensure the deletion of files in order to comply with the user's right to be forgotten.

A report by ENISA (the European Union Agency for Network and Information Security) elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies "outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys".

Cloud providers who take a more proactive approach to this compliance will gain a competitive advantage, according to Patrick Lastennet, Interxion's director of marketing and business development, _ "There is an opportunity for cloud providers who do the legwork with the regulation and tell the customers, 'look, with me, you've got a one-stop shop,'" he says.

Other cloud providers such as Amazon Web Services are offering encryption tools to their enterprise clients to help with compliance. "Enterprises will typically use the cloud to run applications and store data, make sure that everything is encrypted within the cloud, but the management and the key custody is actually completely disassociated from that cloud environment," noted Lastennet.

Safeguarding cryptographic keys in hardware

Encryption is comparably straightforward, with many solutions available on the market. Key management, however, is more complex. Encryption is compromised if an attacker has access to the keys, which may be stored somewhere within the server infrastructure. A Hardware Security Module (HSM) is a piece of security hardware that is designed to prevent exactly that. It safeguards the key material so it cannot be exported in a usable format, preventing any intruder from copying encrypted files and, using the keys, decrypting the data offsite. This scenario is more likely if an attacker can get physical or root access to business servers, such as is the case with insider threats.

When looking at well-regulated examples of consumer data protection, there is no better sector to look to than the financial service industry. In order to safeguard and manage digital keys required for strong authentication, Hardware Security Modules (HSMs) have become a mandatory part of any payment-processing security infrastructure.

Utimaco believes that end-to-end encryption, starting as close as possible to the source of the data, is vital and the only way to prevent unauthorized and unwanted access – regardless of data transfers, storage locations and applicable local laws and regulations.

Installing and utilizing Hardware Security Modules (HSMs) and hardware encryption without backdoors prevent unwanted access to a company's sensitive data and protect data even if a breach has happened. HSMs work with true random number generation, provide encryption and decryption functionalities and allow for the secure identification and authentication of users as well as the integrity of data and code.

In addition, they provide compliance with legal requirements such as FIPS 140-2 (Level 3 or even Level 4) or Common Criteria. The latest HSMs are also suitable for cloud environments where data is not physically stored on the companies' own servers and multiple "tenants" access one single HSM.

Utimaco's Hardware Security Modules are purpose built, physical computing devices designed to protect sensitive data and manage cryptographic keys while ensuring strong encryption methods and providing excellent tamper resistance.

Summary – GDPR: protecting the value of today's most important currency

The EU GDPR is being implemented in order to protect data – as it has become one of modern economies' most important assets. The value of data, for organizations and for the individuals concerned, is growing and it underpins the digital economy. Asking the right questions about the secure use, storage and transfer of data will be mandatory in the future. The GDPR encourages different mechanisms to safeguard data and to comply with the regulations. The overall aim of the regulation is to mandate organizations to manage datasets responsibly and lean, to have an overview of what data is stored when and how and to secure relevant data in order to protect the personal information of EU citizens.

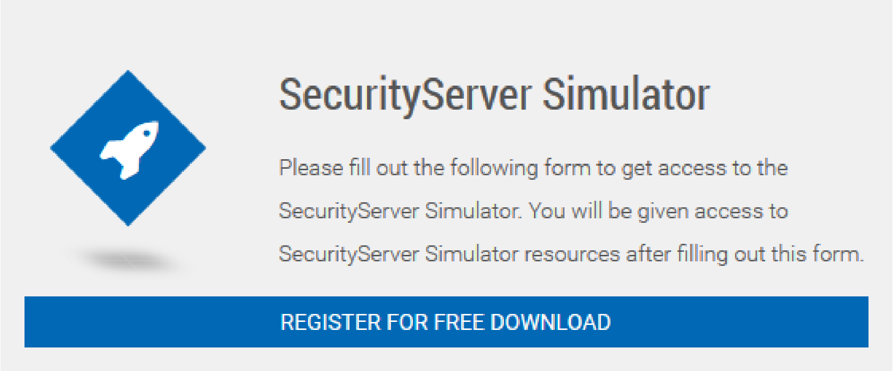
In many sectors, encryption will remain one of the established mechanisms to establish data confidentiality and integrity. Correct implementation will help lessen the impact of the regulation on businesses across Europe and key management is an essential aspect of end-to-end encryption.

About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovations and support the creation of new business by helping to secure critical business data and transactions. Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 170 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit hsm.utimaco.com

Download the Utimaco Software HSM Simulator to get started immediately learning about HSM devices. It is a FREE fully functioning Software version of the Hardware HSM. The download package includes documentation on our product. Here is the link to register for the download.

https://support.hsm.utimaco.com/hsm-simulator



SecurityServer Simulator

Please fill out the following form to get access to the SecurityServer Simulator. You will be given access to SecurityServer Simulator resources after filling out this form.

The Simulator download includes tools for creating user accounts, sample code and libraries for PKCS#11 Microsoft CNG, Java JCE and the Utimaco CXI API to link and test your code. The Simulator will run on a Windows or Linux platform. This is your opportunity to try out the Utimaco HSM technology easily and without initial cost.