WHITE PAPER

Preparing for the General Data Protection Regulation

The emerging requirements and what you can do to get ready for them

While the European Union has had data privacy mandates in place since 1995, those rules are set to see some change. With the approval of the General Data Protection Regulation (GDPR), many organisations will have to start adapting their business approaches, operations, and security policies. This white paper offers a detailed look at some of the most important facets of the GDPR, and it then offers some insights into key approaches that organisations can take now to be well prepared to comply with the new standard when it takes effect.

Introduction: The Evolution of EU Privacy Regulations

In 1995, the European Union (EU) enacted the Data Protection Directive, which created requirements around the processing and transmission of personal data. The Data Protection Directive sought to protect the privacy of EU citizens, and restricted the distribution of sensitive personal data outside EU countries.

Over time, differences in the way member states implemented the law led to inconsistencies in enforcement. As a result, the standard ultimately created complexity, legal uncertainty, and administrative costs for many entities in the EU. In addition, since the release of the directive, the nature of data protection has changed fundamentally, particularly in light of the spread of cloud services, social networking, mobile phones, and so on.

The European Commission developed the General Data Protection Regulation (GDPR) to help strengthen the safeguards around personal data, and also to create a more uniform standard for all EU countries. The GDPR was adopted in April 2016, but the requirements will take effect after two years. When the rule does take effect, the GDPR will replace the Data Protection Directive.

Following is how the European Commission described the nature of the GDPR's changes:

> "The Regulation updates and modernises the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. It focuses on: reinforcing individuals' rights, strengthening the EU internal market, ensuring stronger enforcement of the rules, streamlining international transfers of personal data and setting global data protection standards."[1]

For security and compliance professionals, it will be vital to gain an understanding of these emerging requirements, and how personnel, processes, policies, and technologies may need to be changed to accommodate them.

The following sections offer an overview of some of the key aspects of the GDPR.

Consumer Privacy Rights

GDPR provides privacy protections for the data of individuals based in the EU. Following is an overview of some of the key provisions:

> **Right to be forgotten**. Citizens will have the right to have organisations erase their data and refrain from disseminating this information. For enterprises, this means a consumer's

[1] European Commission, "Fact Sheet: Questions and Answers—Data protection reform", 21 December 2015, URL: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

data needs to be removed not just from production databases, but all backups, archives, and more.

- **Prompt, impartial dispute resolution.** The GDPR provides consumers with clear paths for issuing complaints or handling disputes. Individuals will be granted the ability to exercise their rights free of charge, including objecting to data usage, accessing data, and rectifying complaints. Businesses will be required to respond to complaints promptly.
- **Privacy of children.** The standard will provide specific privacy provisions for children, requiring that consent for children under 13 must be given by the child's parent or custodian. Further, this consent needs to be verifiable.
- **Opt in vs. opt out.** GDPR specifies that the processing of personal data will only be lawful under specific situations, including when "the data subject has given consent to the processing of their personal data for one or more specific purposes."[2] Put simply, business representatives can't assume consent and offer individuals the opportunity to opt out. This will mean many web sites will have to turn cookies (code used to track visitor behaviour) off by default, and only start capturing this browsing data after visitors have explicitly agreed to let the company track their activity. By requiring consent before a business can process personal data for profiling, GDPR will make big data analytics more difficult for many organisations.

Backed by Significant Penalties

Organisations that fail to comply with GDPR will face significant penalties. The GDPR requires member states to specify the penalties for infringements on the regulation, requiring that these penalties are "effective, proportionate, and dissuasive."[3]

The regulation also features steep administrative sanctions, for example, imposing fines of up to 10,000,000 EUR or 2 % of its total worldwide annual turnover whichever is higher. Worse even, if a business is found to be in breach of certain other obligations under the GDPR, the fine may go up to 4% of its total worldwide annual turnover.[4] These fines are applicable whether an organisation has intentionally or inadvertently failed to comply.

Robust Controls

GDPR will require that businesses establish strong controls around personal information and take full accountability for the controls in place. Under GDPR, many organisations will be required to appoint a data protection officer.[5] This includes public agencies, businesses with more than 250 employees, and organisations that specialise in collecting personal data. The regulation provides clear requirements that organisations take steps to protect personal data in order to "prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data."[6]

Staff members will need to review their existing data protection policies and procedures to ensure they are aligned with expected standards. New requirements propose responsibilities not only for data collectors, but also data processors. Businesses will therefore need to take additional steps to vet their partners, and, for example, ensure their cloud providers are establishing the auditable controls required. The framework will also require more visibility into partner contracts to assess privacy policies, and govern whether they are allowed to move data between countries.

Data Sovereignty

As they seek to prepare for GDPR, business leadership can't ignore geographic realities, whether they're running business services on internal infrastructures, external cloud environments, or any combination thereof. This rule applies to controllers or processors based in the EU and to organisations that process data of individuals residing in the EU. In addition, GDPR applies to locations "where the national law of a Member State applies by virtue of public international law."[7]

The reality is that, even when leveraging a cloud service, data will reside in a data center, and that data center will reside in a physical location. Understanding, tracking, and controlling where data resides will be core to ongoing GDPR compliance. These realities are already guiding cloud service providers as they seek to address evolving customer requirements.

Transparency

Transparency is a fundamental theme within GDPR. Having policies in place and executing on those policies will only be a part of the requirements. The regulation requires that data controllers have "transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights."[8]

[2] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 44, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[3] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 92, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[4] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 93, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[5] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 64, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[6] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 60, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[7] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 41, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[8] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing

In event of breaches of personal data, data controllers will need to notify supervisory authorities within 24 hours, and they must also communicate to the individuals whose data has been compromised.[9] Consequently, continuous monitoring will be increasingly critical. When potential violations or breaches occur, it will be imperative to ensure they are detected and addressed quickly. In addition, it will be vital to ensure the controls in place are demonstrable and auditable, both for internal staff and external authorities and auditors.

Addressing Privacy Requirements within an Evolving Business and Technology Landscape

In developing strategies for adapting to GDPR, executives will need to do so within a business and technology landscape that is undergoing fundamental change. Therefore, it will be important to understand how changing dynamics will be influencing these efforts.

It is striking to consider that, just five or ten years ago, it was IT and security teams that were driving not only technology purchases, but standards and usage policies. Now those realities are completely reversed. With the advent of cloud service adoption, the proliferation of mobile technologies, and infrastructure and business service outsourcing, fundamentally new realities have emerged. Now, line-of-business leaders are responsible for almost half of technology purchases.[10] Purchases may be made with or without IT or security involvement, and usage policies are also increasingly being driven from specific business units. Following are some of the implications that IT and security groups are contending with:

- **Eroding control.** In today's environments, IT and security teams are faced with reduced visibility and control over corporate data, including the personal data that may be governed under GDPR. Data may reside in more environments and more diverse systems that aren't under the direct control of an internal IT team.
- **Rapidly expanding devices and device types.** Given the increasing consumerisation of technology—driven by proliferating mobile device usage and IoT technologies like fitness trackers—the number of devices and device types that have to be contended with grows exponentially.
- **Blurring boundaries**. Where in the past a given business would rely on an internal data center for the bulk of its IT requirements, now a typical business will rely on complex ecosystems that are comprised of internally sourced IT systems, virtualised services, private and public clouds, remote disaster recovery sites, managed service providers, business process outsourcers, and more. Consequently, the very concept of a perimeter has been rendered increasingly meaningless.
- **Expanding data volumes**. The proliferation of mobile applications, Internet of things (IoT) initiatives, big data, and so on, are all serving a common purpose: contributing to massively expanding data volumes. For IT and security teams, data continues to grow, and the number of systems, services, and locations that may contain sensitive data expand in kind.

Requirements: Balancing Business Needs and Data Security

As they seek to adapt to GDPR requirements and the changing technology and business dynamics outlined above, IT and security teams will be forced to contend with an increasingly difficult balancing act: Establishing and sustaining strong security controls while supporting rapidly evolving business requirements. Following are two specific areas that will present some of the most pressing challenges:

- **Cloud service support**. As they look to leverage the cost savings, enhanced agility, and other benefits of cloud services, business leaders will continue to look to cloud offerings for more use cases. To support this increased reliance on cloud offerings, IT and security organisations will need to establish and maintain true ownership of data. Whether they're using public, private, or hybrid cloud approaches, they'll need to retain visibility and control over which jurisdictions data will reside in, and ensure that data doesn't get moved outside of regions permitted, whether as a result of a cyber attack, through user error, or as a result of automated backup and recovery processes.
- **Big data and analytics**. To remain competitive, businesses need to leverage big data and advanced analytics. These efforts are vital to enabling improved customer services, enhanced operations, high value offerings and services, and more intelligent planning. To support their businesses, IT and security teams need to establish the systems and services that enable analysts to gain maximum business insights—yet at the same time they need to ensure these analytics implementations don't expose sensitive information. For example, a marketing group within an online retailer may want to leverage demographics and buying and browsing behaviour to tailor promotional offers. IT and security teams would need to establish the infrastructure to support this endeavour, while adhering to GDPR. As a result, they may segregate infrastructures and operations so data for EU customers is only stored and managed within a cloud providers' EU facilities, and establish strong controls to safeguard this data in the cloud providers' premises.

Given the emergence of GDPR, and a host of other privacy mandates and industry regulations, protecting personal data isn't just an objective for security professionals, it's a business imperative. To address this requirement, IT and security teams will need to establish enhanced security controls. Not only will these controls need to address the expanding volume of data, but the increasingly diverse nature of ecosystems that now house corporate data. The following sections offer insights into the key steps needed to establish the controls required.

of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 47, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[9] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 25 January 2012, page 60, 61, URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[10] IDC, "Technology Purchases Funded by Line of Business Budgets Are Approaching Parity with IT-Funded Purchases, According to IDC", 16 February 2016, URL: https://www.idc.com/getdoc.jsp?containerId=prUS41026616

Key Steps for Addressing GDPR and Other Security Requirements

To address the myriad requirements outlined above, it will be more important than ever to adhere to core security principles, with a focus on ensuring auditability, availability, confidentiality, integrity, and accountability. Quite simply, there's no single technology or silver bullet that will address the evolving, challenging security requirements of a global enterprise. Following are some key steps to take to addressing these requirements.

Step #1: Identify Where Sensitive Data Resides

A critical first step will be establishing a complete, accurate picture of where sensitive personal data resides. This is the only way to begin to ensure sensitive data can be secured. As outlined above, however, given the complex IT ecosystems in play today, this is no simple task. In establishing this visibility, following are some of the key questions to consider:

- For each system or service, who has access to data? How will access and other activities be tracked and assigned to specific individuals?
- How many different locations and environments does the data reside in? This includes detailing geographic locations as well as locations within a data center or extended data center (including virtual and cloud environments), and whether data resides on servers (whether file servers, databases, or virtual machines), storage volumes or shares, or disk drives, tapes, or other media.
- How many different data types need to be secured? Are sensitive data elements solely housed in structured data formats, for example as fields in a database, or are they housed in unstructured files like PDFs, images, or word processing documents?
- Where does data get transmitted? This can include data traversing networks between data centers, whether in point-to-point or multi-point environments.

Gaining complete, current answers to all these questions is vital in establishing sound approaches for addressing GDPR requirements.

Step #2: Minimise the Number of Data Repositories Where Possible

Once data locations are identified and understood, it's important to take steps to minimise the number of locations housing sensitive data wherever possible. Particularly with respect to GDPR, if a business could reduce the number of environments or systems that contain personal data, they could potentially significantly streamline their compliance efforts.

Step #3: Safeguard Data Leveraging Encryption and Key Management

For some time, encryption has been emerging as an increasingly important imperative within enterprises, and GDPR will only serve to intensify this demand. Encryption represents an essential way to establish data confidentiality and integrity.

As outlined earlier, the GDPR requires organisations to notify consumers in the event of a breach. However, it also features the following exclusion:

> "The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it." [page 61]

Encryption therefore plays a vital role, offering the possibility of obviating the need for breach notification: If a breach occurs but data was encrypted and keys were protected, a cyber attacker would be unable to decrypt the data and access the actual information. Also, by encrypting data, organisations can ensure that, even if another government issues a subpoena or is secretly accessing a private repository, an organisation can retain control over who can ultimately decrypt the data.

Encryption also represents a strong mechanism for addressing the GDPR's requirements for the consumer's right to be forgotten. By deleting a key associated with a consumer's records, a business could ensure that encrypted data will never be accessed in the clear.

To address the compliance requirements, organizations may need to employ one or more different encryption methods within both their on-premises and cloud infrastructure environments, including the following:

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

In addition, the cryptographic keys generated by encryption processes represent a vital asset, so strong key management capabilities are a critical requirement of any encryption implementation. Quite simply, if keys are vulnerable to loss or exposure, the security benefits of encryption can be negated, and even leave the business exposed to the loss of sensitive and valuable data.

To manage keys securely and effectively, organisations need comprehensive capabilities, including the following:

- Cryptographic processing and acceleration
- Key storage
- Key lifecycle management
- Cryptographic resources management

Further, it is imperative that businesses leverage key management platforms that can scale to accommodate business requirements over the long term. This includes not only supporting increasing volumes of keys, but also expanding volumes of cryptographic transactions. Finally, the platform should offer support for the Key Management Interoperability Protocol (KMIP), which enables organizations to use a single platform to manage keys from different encryption tools, even those from multiple vendors. In this way, businesses can avoid the insecurity, high cost, complexity, and inefficiency associated with managing keys in a siloed fashion.

Step #4: Control Access

Repeatedly, it is weak, static credentials that are exploited to gain unauthorized access to sensitive resources or perpetrate a full-blown data breach. It is therefore essential for organizations to eliminate this vulnerability by establishing strong, multi-factor authentication to any resource that holds value, be it a network, portal, or application.

Strong authentication increases the level of assurance that a user is who they claim to be, enabling businesses to verify the legitimacy of user identities and transactions, and to assign specific activities to individuals. To protect the accounts, data, and intellectual property within their possession, enterprises need to establish controls around the access of employees, customers, partners, and others.

To manage authentication securely and effectively, businesses need comprehensive capabilities, including the following:

- Support for diverse assurance levels. Organizations need to be able to adapt controls to varying use cases and requirements. For example, in consumer and partner scenarios, highly convenient authentication methods may be preferred. On the other hand, higher assurance authentication methods may be required in high risk, high value scenarios, such as business banking applications.
- Unified visibility. Unified audit trails enable administrators to see who is accessing what and when across on-premises, cloud, and virtual resources. These capabilities are vital in supporting auditability and regulatory compliance, while fostering improved administrative efficiency.
- Cloud enablement. Organizations continue to grow increasingly reliant on cloud-based applications, platforms, and infrastructures. This is precipitating a growing demand to implement strong controls for users and administrators attempting to access these critical resources.
- Mobile enablement. The use of tablets and smartphones has become ubiquitous in a number of arenas, including in corporate settings, e-banking, e-retail, and a number of other areas in which sensitive data is shared or accessed. It is critical that organizations establish authentication methods that safeguard access to sensitive services, without adversely affecting the smartphone or tablet users' experience.

Conclusion

Urgent security and privacy requirements aren't anything new for enterprise IT and security teams. However, with the advent of GDPR, the imperatives and scrutiny surrounding the security of sensitive data will continue to expand. The IT and security organisations that take the steps outlined above, will be the ones that position their organisations to quickly and effectively adapt to new GDPR requirements when they take effect.

About Gemalto Data Protection Solutions

Gemalto delivers the breadth of solutions that enable global enterprises to effectively address their evolving business, security, and privacy objectives. With Gemalto solutions, security teams can centrally employ defence-in-depth strategies that deliver holistic, persistent security. Gemalto offers solutions in these areas:

- Encryption. Gemalto data-at-rest encryption solutions deliver transparent, efficient data protection at all levels of the enterprise data stack, including the application, database (column or file), file system, full disk (virtual machine), and network-attached storage levels. In addition, SafeNet High Speed Encryptors deliver proven and certified Layer 2 encryption capabilities that secure data in transit, while addressing business requirements for real-time response and high throughput.
- Key management. With Gemalto solutions, organisations can centrally, efficiently, and securely manage and store cryptographic keys and policies—across the key management lifecycle. These solutions can manage keys across heterogeneous encryption platforms, offering support for the Key Management Interoperability Protocol (KMIP) standard as well as proprietary interfaces. Gemalto offers enterprise key management solutions as well as a range of hardware security modules (HSMs).
- Identity and access management (IAM). Gemalto's portfolio of IAM solutions feature market-leading strong authentication and digital signing products. These offerings enable organisations to secure access to online resources and protect the digital interactions of employees, partners, and customers.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free