gemalto
security to be free

EBOOK

The General Data Protection Regulation

What is it?

Why was it created?

How can organisations prepare for it?

How the General Data Protection Regulation evolved and what it means for businesses

The European Union has had data privacy mandates in place for over twenty years, but those rules are set to see some change in the near future. Approved back in 1995, the Data Protection Directive sought to protect the privacy of EU citizens, and restricted the distribution of sensitive personal data outside EU countries.

More recently, the European Commission developed the General Data Protection Regulation (GDPR) to fortify safeguards around personal data and standardise data protection requirements for all EU countries.

With the approval of the GDPR, organisations will need to adapt their business approaches, operations, and security policies. It will be crucial for security and compliance professionals to understand these emerging GDPR requirements in addition to how personnel, processes, policies, and technologies may need to be changed in order to accommodate them.

"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]

[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

The Origin of EU Privacy Regulations – How Did We Get Here?

As time progressed since the EU originally enacted the Data Protection Directive in 1995, differences in the way member states implemented the law led to inconsistencies in enforcement. Ultimately, the standard created complexity, legal uncertainty, and administrative costs for many entities within the EU.

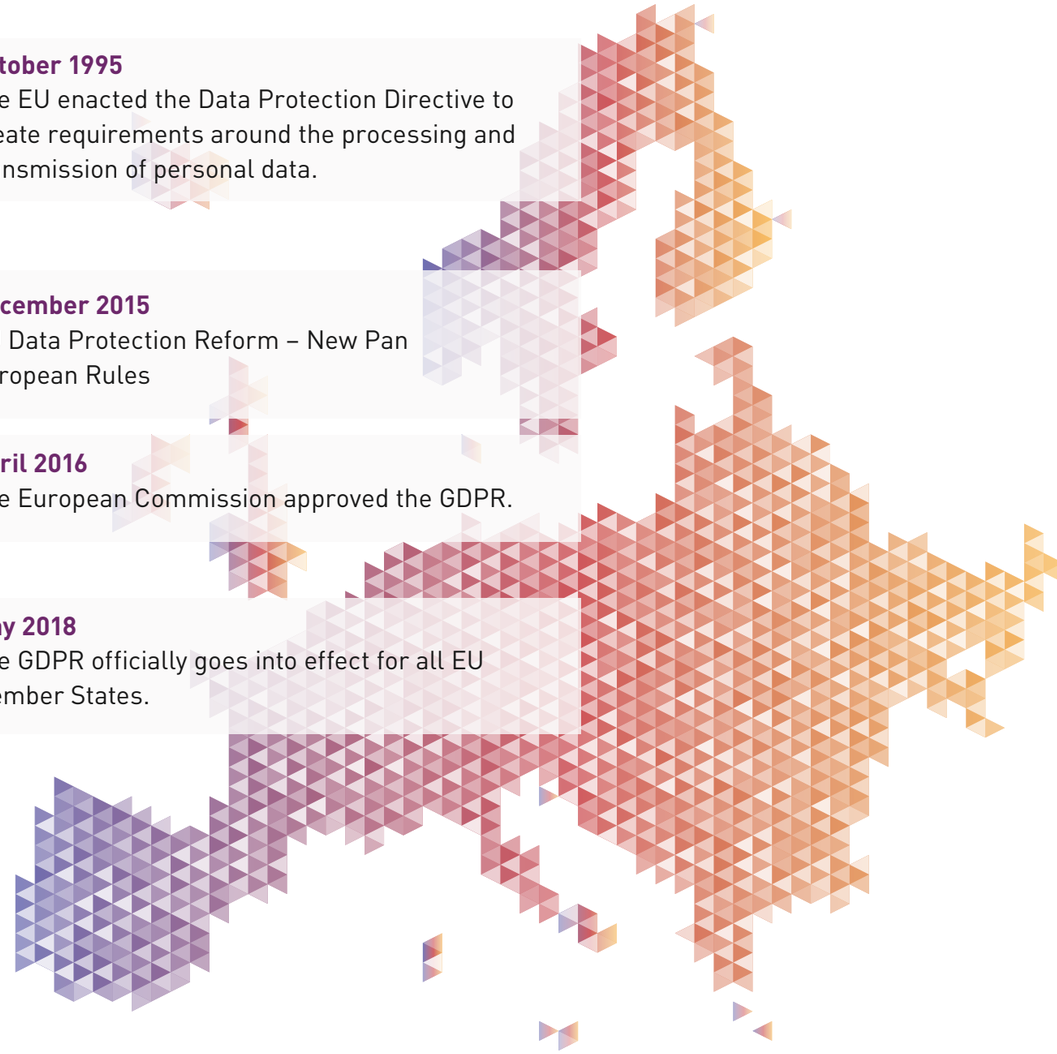
Subsequently, the European Commission developed the GDPR to not only strengthen the safeguards around personal data but create a more uniform standard for all EU countries. The GDPR was adopted in April 2016, but the requirements will not take effect for another two years. When the rule does take effect, it will replace the Data Protection Directive.

October 1995
The EU enacted the Data Protection Directive to create requirements around the processing and transmission of personal data.

December 2015
EU Data Protection Reform – New Pan European Rules

April 2016
The European Commission approved the GDPR.

May 2018
The GDPR officially goes into effect for all EU Member States.



Key Aspects of the General Data Protection Regulation

1. Consumer Privacy Rights

> **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 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.

> **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.

> **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 processing of their personal data for one or more specific purposes."[2] Essentially, business representatives cannot assume consent. This will mean many web sites will have to turn cookies (code used to track visitor behaviour) off by default, and only start tracking after visitors have explicitly agreed.

[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

2. Backed by Significant Penalties

> Organisations that fail to comply with GDPR will face significant penalties.

> The regulation features steep administrative sanctions, including substantial fines that are applicable whether an organisation has intentionally or inadvertently failed to comply.

3. Robust Controls

> GDPR will require that businesses establish strong controls around personal information and to take full accountability for the controls in place.

> 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."[3]

> Staff members will need to review their existing data protection policies and procedures to ensure they are aligned with expected standards.

4. Data Sovereignty

> This rule applies to controllers or processors based in the EU and to organisations that process data of individuals residing in the EU.

> Understanding, tracking, and controlling where data resides will be core to ongoing GDPR compliance.

5. Transparency

> 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."[4]

> Continuous monitoring will be increasingly critical. When potential violations or breaches occur, it will be imperative to ensure they are detected and addressed quickly.

[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 60, URL: http://ec.europa.eu/justice/dataprotection/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 47, URL: http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf

Key Steps for Addressing GDPR

1. Identify Where Sensitive Data Resides

A critical first step will be establishing a complete, accurate picture of where sensitive personal data resides.

> 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.

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.

3. Safeguard Data Leveraging Encryption and Key Management

Encryption represents an essential way to establish data confidentiality and integrity. In fact, the GDPR will only intensify the demand for encryption.

> Encryption offers the possibility of obviating the need for breach notification, as required by the GDPR unless proper technological protection measures are implemented. 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.

> 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.

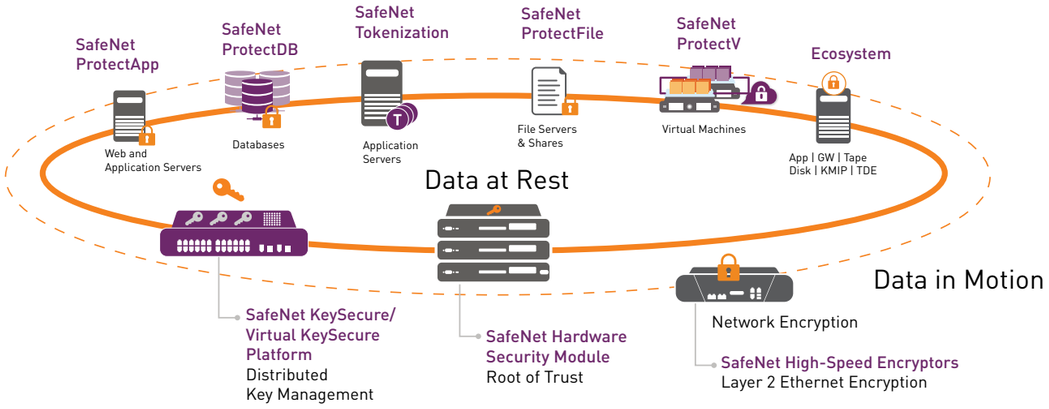
> By deleting a key associated with a consumer's encrypted records, a business could ensure that data will never be accessed in the clear.

4. Control Access

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

Look for an experienced vendor who can offer you a complete solution.

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 that address GDPR requirements

> **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 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.

ABOUT GEMALTO'S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilising innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organisations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

GEMALTO.COM