FORCEPOINT
POWERED BY Raytheon

GDPR – A legislative milestone for a digital age

BY NEIL THACKER, INFORMATION SECURITY & STRATEGY OFFICER, EMEA FORCEPOINT™

The clock is officially ticking for organisations to get their data protection policies in order now that the General Data Protection Regulation (GDPR) has been approved and is set to replace the previous EU Data Protection Directive.

The new regulation will come into effect in May 2018 and will require organisations to put a much stricter focus on data protection. The headline items for organisations that collect or process EU citizen records are:

- They must notify their supervisory authority of a data breach within 72 hours.
- The subject will have the right to retract consent, request data erasure or data portability.
- They may face fines of up to 4% of their worldwide turnover, or €20 million for intentional or negligent violations.

These increased sanctions mean it is vital that this new law be fully understood by a number of key stakeholders within the organisation, and that organisations start preparing to comply with the new regulations as soon as possible.

There are five key steps to help organisations perform a basic assessment of their current data protection strategy and to identify any potential gaps that need filling prior to a more comprehensive view of the GDPR.

1. IDENTIFY OBLIGATIONS

The first task for any organisation must be to identify whether they are considered a data controller or processor. They must review the relevant obligations these carry, such as issuing notice to citizens and maintaining relevant consent from the data subject.

Organisations should make it common practice to regularly review existing and new business processes to identify personal identifiable information (PII). They should identify where this data resides – whether it's at-rest, in-motion and/or in-use and maintain a record of processing activities and understand how this data is protected.

2. PROTECT PII

Once PII has been identified, organisations must then ensure that they adequately protect this data. Encryption and access control are common control standards, but managing encrypted data across multiple business processes is a hugely difficult task.

Data sovereignty and data lifecycle management are key to helping organisations ensure that EU citizen data is processed and stored appropriately. In addition to these responsibilities, they also need to manage data flows to approved third party processors, monitor for accidental data leakage from negligent or malicious employees and protect against data theft from external attackers.

3. DETECT BREACHES AND THEFT

If an organisation does suffer a loss of data then it is vital to detect the breach and identify if PII records were lost or stolen. If they have, the organisation will be required to notify the necessary authorities within 72 hours of the discovery to initiate a full investigation.

The investigation will focus on identifying the source and destination of the breach through event and incident information from Data Leakage Prevention (DLP) and Data Theft Prevention (DTP) tools. Data forensics will then help to pinpoint the stolen data, at which time the organisation will be required to issue notice to any affected data subjects.

"There are increased obligations on controllers and processors. Individuals are put in a stronger position, and critically for business, increased enforcement powers, fines, and rights of individuals to take action."

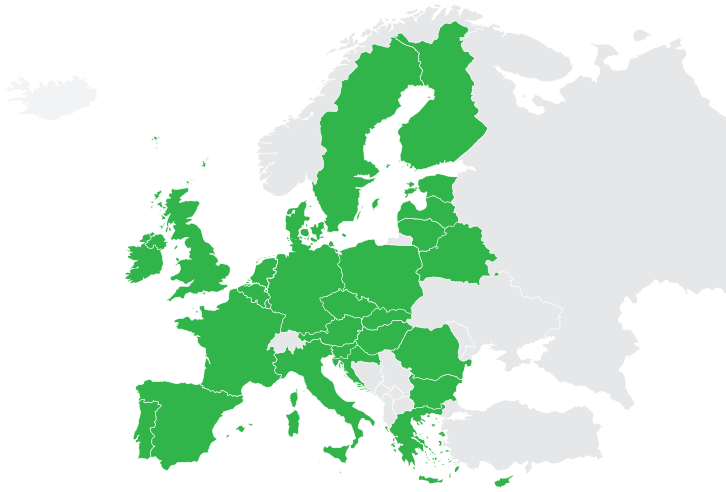
— ROSEMARY JAY, SENIOR CONSULTANT ATTORNEY, HUNTON & WILLIAMS

4. RESPONSE PLANS

Incident response is critical to protecting data and protecting EU citizen data. In addition to the mandatory data breach notification requirement, organisations must also ensure they have implemented an effective incident response plan. This plan must have been regularly tested to ensure that employees involved in a data breach response are familiar with and fully understand the new legislation and communication process in order to report a breach.

5. RECOVERY MANAGEMENT

In the aftermath of a data breach, organisations must ensure that they maintain ongoing communication with the relevant authorities. This will ensure secondary loss factors are managed and keep affected data subjects regularly informed.



ABOUT FORCEPOINT

Forcepoint's portfolio of products safeguards users, data and networks against the most determined adversaries, from accidental or malicious insider threats to advanced outside attacks, across the entire threat lifecycle.

Specific to GDPR, Forcepoint provides organizations with deep visibility into how critical data is being processed across their infrastructure; on-premises, in the Cloud or within their increasingly remote workforce.

Forcepoint's data protection and insider threat technologies not only provide the ability to monitor, manage and control data at rest, in use and in motion, but they also utilize user behavior analytics and machine learning to discover broken business processes and identify employees that elevate risk to critical data.

THERE ARE THREE CORE AREAS WHERE FORCEPOINT'S SOLUTIONS CAN HELP ORGANIZATIONS MEET THE REQUIREMENTS OF THE GDPR:

- Inventorying personal data, whether as part of the initial scoping of a compliance program or to support the operational duties of controllers, processors or responders, including dealing with subject access requests or data incidents.
- Mapping personal data flows across the organization that expose broken business processes and unsanctioned IT or highlight supply chain activity that puts critical data at risk. This clear visibility allows organizations to implement management and control of personal data flows using mechanisms such as authorization, policy-based encryption, notification and blocking to mitigate risk.
- Leveraging behavioral analytics and risk modelling to rapidly detect high risk employee activity (malicious or compromised) and broken business processes that put critical data at risk, as well as enabling a quick and decisive response, which often lets organizations get ahead of the breach itself.

FOR MORE INFORMATION ON GDPR, VISIT: WWW.FORCEPOINT.COM/GDPR

CONTACT
www.forcepoint.com/contact