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."

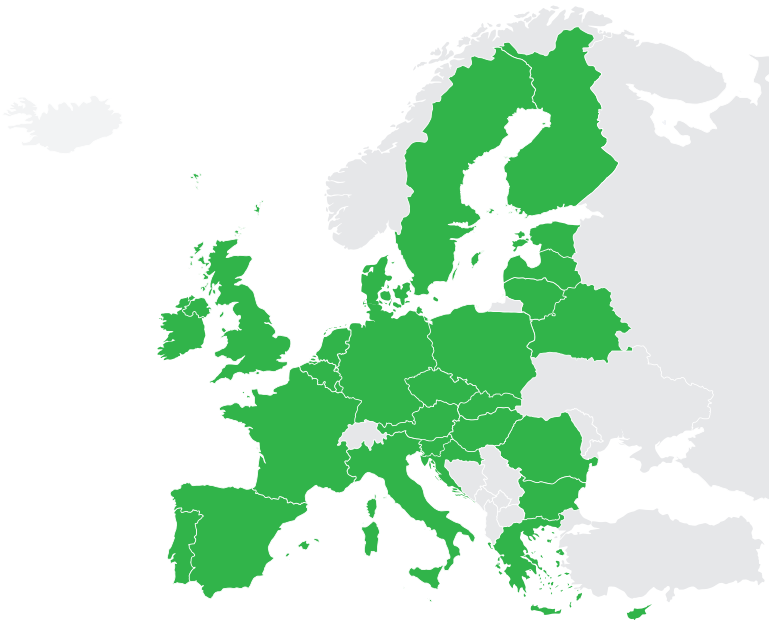
— ROSEMARY JAY, SENIOR CONSULTANT ATTORNEY, HUNTON & WILLIAMS

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.



Data protection and the safeguarding of EU citizen data has always been an important requirement for organisations and the impending GDPR places even greater emphasis on the value of this data. It is therefore more important than ever for organisations to fully understand their role and apply the appropriate security controls that allow them to identify and protect this data. Having an established data breach plan in place will then help organisations be familiar with the detect, response and recovery phases to ensure they limit the effect of the attack and have the relevant people, processes and technology in place to continually deal with this new legal and regulatory requirement.

For more information on GDPR, visit: www.forcepoint.com/GDPR

"A new requirement exists to notify your supervisory authority of a data breach within 72 hours of discovery of the breach. There's also a requirement to notify individuals where the breach is likely to present a high risk to the individual."

— JAMES HENDERSON, ASSOCIATE, HUNTON & WILLIAMS

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT