The General Data Protection Regulation (GDPR)

Get the facts and prepare your business

LogRhythm®

The Security Intelligence Company

The existing legislative landscape for data protection across the European Union is fragmented, causing confusion to individuals and businesses. The current regulations in place to protect EU citizen data are out of date and have long been overtaken both by technology and by the way data is stored and secured.

The outgoing legislation—the EU Data Protection Directive 95/46/ec—came into force in 1995 when the internet was still in its dial-up infancy and mobile phones were far from smart. Since then, the way data is collected and used has changed fundamentally, yet the same outdated data protection laws have applied.

The incoming General Data Protection Regulation (GDPR) will address the gap and make EU privacy and data laws fit for purpose in the digital age—harmonising data protection laws in the EU. The EU believes common, shared laws will bring better transparency to help support the rights of individuals and grow the digital economy.

It's important to note that the GDPR is a regulation and not a directive. This means that when it comes into effect in spring 2018, it will be directly applicable in all EU member states as a single law. There will be no need to implement legislation in individual countries. From May 2018, the GDPR will apply, no questions asked.

In this paper, we'll look at some of the key principles of the GDPR, what those principles mean for security and compliance teams and how you can prepare your organisation for the 2018 deadline. Make no mistake: The GDPR will require organisations that collect and process EU citizen data to undertake major operational reforms.

The GDPR is a huge body of legislation, so this paper will focus on some specific areas where security, communications and compliance specialists will need to prepare.

When is it coming?
The GDPR was adopted on 27 April 2016 and it will become law on 25 May 2018, following a transition period. This means companies and organisations around the world have less than two years to get ready for the changes that affect how personal data is transferred to and from, as well as within, the EU.

Who does it affect?
Put simply, it affects any organisation that does business with an EU organisation or individual. Non-EU organisations that collect and process the personal data of European citizens will also be subject to compliance with the new law and will need to apply for a certification that their processes meet EU data privacy standards. No matter where you are based in the world, if you want to do business within the EU, you will need to comply with the GDPR.

What about Brexit?
The process for exiting the EU will take longer than two years to complete, so the UK will still be a part of the EU when GDPR becomes law. After that, the position for the UK is less clear and depends on the will of the government.

However, if UK businesses want to do business in the EU, they will need to comply with the GDPR. The regulation is universally applicable.

For EU countries, post-Brexit UK organisations will be affected by the GDPR just like any other non-EU entities.

How will the GDPR affect security professionals?

The full scope of the GDPR is huge and broad ranging. In this paper we will consider two key areas of the regulation that will affect security and privacy professionals:

- Reporting data breaches
- Data protection by design

These two areas will call on organisations to analyse their operations ahead of the introduction of the GDPR and respond in two areas:

- Accountability to meet reporting requirements
- Compliance with privacy best practice

Reporting data breaches

The incoming regulations raise the bar in dramatic fashion on the need for data breach reporting. Organisations must urgently review and put in place operational and technological arrangements to satisfy the GDPR.

Identifying when and understanding how attackers got through the organisational defences are now fundamental to a business' operations. Given the considerable penalties, the failure to champion this capability could end up being financially crippling to companies under the GDPR.

What does the GDPR say?

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4, definition 12).

On the position of reporting the breach, the regulation states: "As soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it..." (Article 33).

What does this mean?

Directive 95/46/ec made no specific mention of data breaches in its many paragraphs of regulations. The GDPR is different. It sets a clear definition of what constitutes a "personal data breach", how an incident needs to be reported to the relevant authorities and the penalties for failing to do so.

Any organisation suffering a data breach will be required to report it to the national data protection body and also notify any affected customers swiftly. That means businesses will need to ensure they have the technology and processes in place to be able to both detect and report any breaches in compliance with these stringent new requirements.

Under the GDPR, notice must be provided by the data controller, as noted previously, "without undue delay", preferably within three days of detection.

The notification to the relevant data protection authority must contain at minimum:

- A description of the "nature of the personal data breach", including the number and kinds of data records affected
- The data protection officer's contact information
- An outline of the "likely consequences" of the breach
- A description of how the data controller proposes to address the breach, including "measures to mitigate its possible adverse effects"

Data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

In the event of a breach, the data processor must report it to the relevant data controller, but he or she otherwise has no reporting obligation under the GDPR. However, if the controller determines that the breach is likely to result in a "high risk to the rights and freedoms" of data subjects, he or she needs to communicate this to the individuals affected "without undue delay".

If a data controller does not submit the notification within 72 hours, then a "reasoned justification" must be provided for the delay.

The penalties for failing to report breaches, without reasoned justification, will be set at a maximum of €20m or four per cent of an organisation's annual revenue, whichever is greater.

Given the cost implication, there's a compelling argument for organisations to ensure they have the systems and processes in place to identify a breach, gather the information they need together and report details without undue manual effort.

Data protection by design

One of the key principles of the new legislation is the concept of 'data protection by design'[1], also known as privacy by design. This means organisations will be subject to a specific obligation to include data protection considerations into a service, process or product from the onset, and not as an afterthought, as is often the case.

What does the GDPR say?

Article 25 of the GDPR is dedicated to the principle of data protection by design. The GDPR states: "The controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default."

The regulation proposes this could be achieved by:

"... minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features" (78).

What does this mean?

Under the GDPR, data protection and processing safeguards must become part of the DNA of all systems and processes. Privacy must be one of the pillars of new application development and new processes, and not an afterthought or a last-minute workaround. This is a major consideration under the GDPR and one for which organisations need to prepare. It is a principle that businesses need to be thinking about now, not later.

This principle is another example of how the GDPR has responded to the changing nature of data protection since the inception of the previous direction, which didn't recognise the concept of privacy by design. Directive 95/46/ec did not state that privacy should be a significant consideration at any point in the design process for new products or the organisational measures for new processes.

The concept of privacy by design has been around for a number of years and the UK Information Commissioner's Office (ICO) has published useful guidance on the subject[2].

Data protection by design is based on seven "foundational principles":

- Proactive not reactive, preventative not remedial
- Privacy as the 'default' setting
- Privacy embedded into design
- Full functionality: positive-sum, not zero-sum
- End-to-end security: full lifecycle protection
- Visibility and transparency: keep it open
- Respect for user privacy: keep it user-centric

Organisations are encouraged to reduce the amount of personally identifiable information stored, removing certain types of data. In addition, organisations will need to review and reduce data retention times and ensure that "only personal data which are necessary for each specific purpose of the processing are processed".

Data protection impact assessments (DPIA) may be required in many circumstances, especially for organisations with systems and processes that are likely to result in a high risk to data subjects' rights.

A DPIA should "evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with [the regulation]". Forward-thinking organisations should undertake DPIAs early on during system and process design. Identifying problems early on can help reduce costs later and avoid potential damage to reputation.

One important new principle introduced by the GDPR and closely related to data protection by design is the concept of 'pseudonymisation'. This is defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information"[3]. The identifying data should be maintained in a separate location as part of best practice.

The application of pseudonymisation to personal data can help reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations.

[1] https://en.wikipedia.org/wiki/Privacy_by_design
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/
[3] GDPR (Definitions) Article 4 (5) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

‘Pseudonymisation’ is defined as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information”.

Rising to the challenge

The GDPR is a major change to the way EU personal data needs to be processed. Remember: The GDPR is universally applicable. If organisations want to do business in the EU, they will need to comply with the GDPR. To respond and be ready, security teams need to develop a number of capabilities to meet the demands of the GDPR around breach reporting and data protection by design.

Accountability for breach reporting

Research published in May 2016 revealed that 65 per cent of large companies experienced a breach in the previous 12 months, with a quarter of those organisations weathering attacks on a monthly basis[3].

Strategies that focus only on keeping attackers out are failing. Once an attack penetrates a corporate system, it can go undetected, giving the business little chance to respond.

Recent research which studied 691 data breach investigations worldwide, spread across all industries, illustrates the problem[4]. In all, 71 per cent of compromised victims did not detect the breach themselves.

Furthermore, it took organisations an average of 87 days—nearly three full months—to detect a compromise. Once detected, it took organisations an average of a week to respond. Clearly this represents a huge risk in light of the GDPR’s reporting requirements and the possible penalties that could follow.

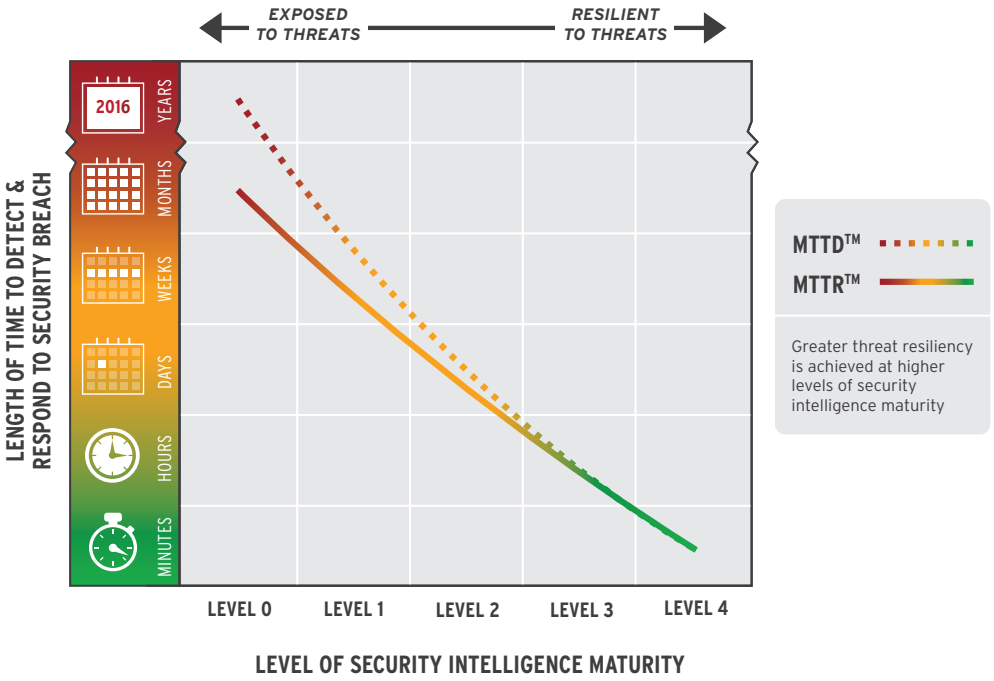
Keeping threats out is important, but forward-thinking organisations acknowledge they will not always succeed. Breaches are inevitable. Leading chief information security officers (CISOs) have become focused on two metrics relating to this new approach to security: mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR). With these two measures, organisations can understand how they are protecting their vital data, not just an organisation’s perimeter.

Under the old way of thinking, few resources are targeted at understanding threats that penetrate the system or measuring the response. If a company spends all its resources building and maintaining defence systems, it has nothing left to detect and respond to attacks that succeed.

Checklist:
Reporting data breaches

The GDPR will require companies to develop or update internal breach notification procedures to meet the 72-hour reporting requirement:

- Timely detection of breaches
- Reporting and alarms
- Mitigation through automation
- Investigation capabilities (case management and forensics)



[4] Two-thirds of UK firms suffered cyber attacks in the last year http://www.itpro.co.uk/security/26496/two-thirds-of-uk-firms-suffered-cyber-attacks-in-the-last-year
[5] Surfacing Critical Cyber Threats Through Security Intelligence: A Reference Model for IT Security Practitioners https://logrhythm.com/pdfs/whitepapers/lr-security-intelligence-maturity-model-ciso-whitepaper.pdf

"Businesses need to be working to make privacy a fundamental part of their technological and organisational set-up, and the countdown timer is already ticking."

Compliance and data protection by design

Compliance with the GDPR promises to be a major operational and technological overhaul for organisations. Every company that plans to do business in the EU needs to have analysed and understood what the GDPR demands of its organisation and develop a programme for achieving compliance. That analysis needs to start immediately.

Companies must also assign adequate budget to meet the need for compliance with the data protection regulations, which become law in May 2018. The penalties for failing to meet them are stark.

Organisations must also hire a data protection officer (DPO) if they meet the criteria to do so. The DPO's responsibilities include ensuring compliance with the GDPR and providing relevant training within the organisation.

The GDPR will call for the introduction of a number of organisational changes to how data is managed:

- Data protection (privacy) risk assessments will be introduced
- Data retention must be reported
- The amount of personally identifiable information should be reduced
- Certain kinds of data should be removed
- Data retention periods should be reduced

To meet potential contractual requirements, organisations may need to demonstrate compliance with all applicable EU laws and show compliance using existing industry or security best practice mandates such as:

- ISO 27001:2013
- PCI-DSS
- GPG-13
- BSI IT Grundschutz

Having control and accountability where raw data and metadata are stored will be an important competency to meet controls around GDPR's international data transfer. With this in mind, it is important to develop capability within the organisation for data segregation and role-based access control with full audit activity and tamper detection.

The GDPR has also defined and increased the range of personally identifiable information (PII). As a result, enterprises may wish to reduce the chance of PII leaking by masking collected log data.

Finally, and crucially, as with all cybersecurity practices, workplace education will play an important part in ensuring compliance with the GDPR. Customer data is managed in areas outside the IT department—from marketing to HR to customer services to finance. Staff members need to understand the core principles and responsibilities of data protection and privacy under the GDPR. They also need to understand how the implications of failing to do so could affect the organisation.

To prepare for the GDPR, organisations need to be considering these areas now. The principle of data protection by design calls for compliance from the ground up, not as an add-on. Businesses need to be working to make privacy a fundamental part of their technological and organisational set-up, and the countdown timer is already ticking.

Checklist:
Compliance and data protection by design

The GDPR will require companies to rethink how data protection and privacy are met and managed by the organisation:

- Analyse gap between current and mandated position
- Assign required budget and resources
- Assign a data protection officer if criteria are met
- Align with best-practice mandates
- Review and update data-handling procedures
- Develop a workplace education programme

Learn more about how to prepare for GDPR

Talk to LogRhythm's experts about the EU's coming GDPR and about your information security and compliance needs.

Find us

LogRhythm Ltd.
Clarion House
Norreys Drive
Maidenhead
SL6 4FL
UK

Contact us

Tel: 01628 918 300
Email: europe@logrhythm.com

"From marketing to HR to customer services to finance... staff members need to understand the core principles and responsibilities of data protection and privacy under the GDPR."

Glossary

General Data Protection Regulation:
A regulation coming into effect in May 2018 to replace Data Protection Directive 95/46/ec and strengthen and harmonise the data protection rights of EU citizens.

Data Protection Directive 95/46/ec:
A 1995 directive on the protection of individuals which regulates the processing of personal data in the EU. To be replaced by the GDPR.

Personal data breach:
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pseudonymisation:
The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

Data protection officer:
A privacy expert who must operate independently to make sure an organisation is following procedures and policies set out in the GDPR.

Data protection by design:
A key GDPR principle that states organisations will be subject to a specific obligation to include data protection considerations into a service, process or product from the outset.

Data controller:
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor:
Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal data:
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly.