The General Data Protection Regulation (GDPR)

KEY THEMES AND CHALLENGES OF THE GDPR

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

GDPR – A legislative milestone for a digital age

The countdown has started for organizations to get their data protection programs in order, now that the GDPR approaches its enforcement date, officially replacing the outgoing EU Data Protection Directive.

The new regulation will be enforceable from 25th May 2018 and will require organizations to put a much stricter focus on data protection. The headline items for organizations that collect or process EU resident records are as follows:

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

These increased sanctions have created urgency around the GDPR and have prompted key executive stakeholders within organizations to prioritize personal data protection. The same stakeholders have asked processors and sub-processors to mature their preparation in order to comply with the new regulations as soon as possible.

On 25 May 2018, less than 50% of all organizations impacted will fully comply with the GDPR.
—Gartner*

*Gartner, GDPR Clarity: 19 Frequently Asked Questions Answered, by Bart Willemsen, 29 August 2017

Top three misconceptions around the GDPR

Rosemary Jay, Senior Consultant Attorney from Hunton & Williams, ranks her top 3 misconceptions around GDPR.

1
GDPR is a negative piece of legislation

These changes are not due before time: we needed to updated the way we regulate personal information as we move towards a digital economy. It will engender trust and provide good practises that will benefit both the individuals and the business. It will give a real impetus to businesses to "spring clean" their data and the imperative to comply with retention schedules, put in place psuedonominization and look at data in a new way.

2
It is somebody else's responsibility

It is not just the responsibility of the Data Protection Officer (DPO) – the business is ultimately the data controller. This is a significant corporate responsibility that needs to be owned by the board. If it is a risk issue, it is no longer a low level concern. You cannot outsource your responsibility, the organization must take real ownership.

3
GDPR does not affect the public sector

There are differences for the public sector in the UK: policing and criminal justice are covered by a different law. However, the core obligations of accountability and notice apply equally to the corporate and public sector.

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

Listen to Rosemary discuss her **top GDPR misconceptions**

Five key steps to help organizations perform a basic assessment

Security frameworks are a good way to align information security and data protection programs, and preparing for GDPR is no different. Using the common **NIST Cyber Securiy Framework** functions, we identify five key steps to help organizations perform a basic assessment of their current data protection strategy and identify any potential gaps that need fulfilling prior to a more comprehensive view of the GDPR.

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

1

IDENTIFY OBLIGATIONS & SCOPE

The first task for any organization must be to identify whether they are considered a data controller or processor. They must review the relevant obligations these titles carry, such as issuing notice to citizens and maintaining relevant consent from the data subject. Organizations should make it common practice to regularly review existing and new business processes to identify personal data. They should identify where this data resides — whether it's at rest, in-motion and/or in-use — maintain a record of processing activities, and understand how this data is protected.

With one law on data protection across all 28 member states, organizations no longer have to manage different data protection approaches per market. The European Commission estimates this will save businesses around €2.3 billion annually.

—Osterman Research

2
PROTECT PERSONAL DATA

Once personal data has been identified, organizations must ensure they adequately protect this confidential data. Encryption and access control are common control standards, but managing encrypted data across multiple business processes is an enormously difficult task.

Data sovereignty and data lifecycle management are key to helping organizations ensure that EU resident data is processed and stored appropriately. In addition to these responsibilities, organizations need to manage data flows to approved third party processors, monitor for accidental data leakage from workforce accidental or intentional misuse, and protect against data breaches from external attackers.

3
DETECT BREACHES

If an organization does suffer a breach of data then it is vital to detect the breach and identify if personal data was affected. If affected, the organization will be required to notify the necessary supervisory authorities within 72 hours of the discovery, in order to initiate a full investigation.

The investigation will focus on identifying further details of the breach through event and incident information from tools such as Data Loss Prevention (DLP). Data forensics will help pinpoint the data involved in the breach, at which time the organization may also be required to issue notice to any affected data subjects.

GDPR HAS A GLOBAL REACH...

Whilst awareness of the GDPR is increasing, the broader impact is still misunderstood: **any** global organization that holds or processes EU resident data will be subject to the regulation. This can affect organizations in the United States, Mexico, India, Australia... essentially any international organization that does business with the EU.

Watch our webcast,
"The Global Impact of GDPR"

The GDPR is already achieving its objective of turning European data protection into a framework for global compliance.
— Eduardo Ustaran,
Partner, Hogan Lovells

4
RESPOND WITH A PLAN

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

5
RECOVER FROM THE BREACH

In the aftermath of a data breach, organizations must ensure that they maintain ongoing communication with the relevant authorities. This will ensure secondary loss factors are managed and ensure the affected data subjects are regularly informed. Organizations must also work closely with their Data Protection Officer (DPO) to ensure additional communications are managed across multiple jurisdictions if the breach has a global impact. Data protection and privacy laws are undergoing change the world; it is imperative for security professionals to work closely with the DPO to understand additional steps needed to recover the organization and become resilient to the next wave of threats.

The EU GDPR is dream and a nightmare scenario for CISOs

The initial challenge of the GDPR is a daunting one, as organizations around the world receive further clarification on their responsibilities as either data controllers, data processors or both.

A GDPR program can be extensive in its implementation and requires a good understanding of the regulation and the legal text. As the regulation is non-prescriptive and therefore outcome-based, it requires a good level of data protection maturity and a tried and tested understanding of an organization's processing activities, including an understanding of all 3rd-party personal data processors and sub-processors.

This involves reviewing customer information whereby goods, services and/or profiling is a business activity for on-site and cloud-based systems but also involves a review of employee personal data activities. This can typically encompass upwards of 100+ systems for organizations to revisit and review existing and any new organizational and technical controls. As a member of the GDPR program team at Forcepoint, the program has been an informative experience and further demonstrated the need for strong data protection and communication skills across the organization. It has been a challenge but one that comes with immense rewards.

Neil Thacker
Deputy CISO,
Forcepoint

Listen to Neil Thacker participate on the (ISC)2 webcast, **"GDPR: Countdown to Day0"**

How Forcepoint can help

Forcepoint provides organizations with deep visibility into how personal data is being processed across their infrastructure; on-premises, in the cloud or within their increasingly remote workforce. Forcepoint can support organizations towards GDPR compliance with products that can help you **Identify, Protect, Detect, Respond** and **Recover**.

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.
- **Rapid detection and response** by leveraging behavioral analytics and risk modelling to 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 lets organizations get ahead of the breach.

Forcepoint technology mapped to the 5 pillars of the NIST security framework

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Forcepoint DLP	•	•	•	•	
Forcepoint UEBA			•	•	
Forcepoint Insider Threat			•	•	•
Forcepoint Cloud Access Security Broker	•	•	•		
Forcepoint Web Security		•	•		
Forcepoint Email Security		•	•		
Forcepoint Next Generation Firewall		•	•		

For more information, read the **Forcepoint GDPR Product Mapping Overview**

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact

[EBOOK_FORCEPOINT_GDPR_EN] 800005.101317