What is GDPR and What Does Your Organization Need to Do to Comply?

The clock is ticking on the implementation of a major piece of new European Union (EU) legislation that will affect all companies doing business in Europe. On May 25, 2018, the General Data Protection Regulation (GDPR) will come into existence, and will cast a very wide net indeed. It will apply to all companies with operations in the region AND to companies with a website or app that captures and processes EU citizen data.

While GDPR is everywhere in security and privacy news these days, much of the coverage focuses on GDPR at a high-level, covering such topics as implementation timeline, potential fines and 'the Right to Erasure'.

While important, those topics just scratch the surface of legislation that is so broad in scope, it affects a multitude of issues ranging from corporate governance to consent rights.

Due to the complexity of the legislation and the fact that not all of the details have been finalized, the readiness of companies is quite varied. Some companies have grasped the basics, others are in advanced stages of meeting their compliance obligations, while others have taken the 'wait and see' approach that will force them to scramble at the last minute.

Unless your organization enjoys risks and has the legal resources to support them, scrambling at the last minute is not the way to go. Failure to comply with GDPR is likely to result in substantial fines: as much as four percent of an enterprise's worldwide revenue. Two pain points stand out: a requirement to notify EU authorities within 72 hours of a breach, and another to prove your security approach is state-of-the-art.

Over the last year, the (ISC)^2 EMEA Advisory Council has consulted our professional membership to measure the readiness of organizations and security departments for GDPR, and to highlight the challenges they are facing in the effort to become compliant by May 2018. The council established a Task Force that brings people together who are actively working on implementation projects either on monthly international calls or in face-to-face workshops hosted within (ISC)^2 Secure Summits.

This effort reveals that many organizations have underestimated the workload required and failed to allocate accountability and resources adequately. Too many have assessed it as an IT/ICT or security department concern, when the understanding of value, along with why and how personal data is processed, sits within the business functions.

The first barrier reported by (ISC)² members working on compliance projects, was an inability to get projects off the ground due to a lack of engagement from business stakeholders, a concern which has persisted throughout 2017.

Wherever your organization is on its route to compliance, this document will help you to begin to understand GDPR and your company's compliance obligations.

What is GDPR?

The European Parliament adopted GDPR in April 2016, replacing a data protection directive approved in 1995. The new law carries strict provisions that require businesses to protect the personal data and privacy of EU citizens for all data transactions. The GDPR also regulates the export of personal data outside the EU.

The provisions are consistent across all 28 EU member states, meaning that companies must comply with just one standard in the EU. However, that standard is quite high and will require companies around the world to make a large investment to meet it and maintain it.

A recent survey by Spiceworks suggests that only nine percent of IT/ICT professionals in the United States have an understanding of what GDPR entails and how it affects their businesses. In contrast, the survey found that 43 percent of IT/ICT people in the UK and 36 percent in the rest of the EU are informed and prepared for the legislation.

The knowledge gap in the US might be due to the belief that many IT/ICT pros don't believe GDPR will affect their organizations, wrote Spiceworks analyst Peter Tsai. By comparison, only 3 percent of IT/ICT pros in the UK and 9 percent in the EU believe their company will be exempt from GDPR.

While GDPR goes beyond the remit of the IT/ICT or security department, this lack of awareness is a strong indicator of corporate preparedness in the US.

Spiceworks surveyed nearly 800 IT/ICT professionals in the United States and Europe.

Who Does GDPR Apply to?

GDPR applies to any organization that collects and processes data of EU citizens, even if the processing is done outside of the EU. GDPR classifies organization as 'controllers' or 'processors.'

Many organizations play both roles depending on the process involved.

Controllers determine how and why personal data is processed, while processors act on the behalf of controllers.

If you are a processor, GDPR places specific legal obligations on you. For example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved — GDPR places further obligations on you to ensure your contracts with processors comply with GDPR.

Key areas of the legislation are privacy rights, data security and control, and governance. For both processors and controllers, the legislation details how these areas should

be managed, by requiring documented inventories of personal data, workflows, policies for updating or retiring data stores, processes to support the right to erasure, and more. These requirements constitute much of the heavy workload of companies striving to develop a much better understanding of their processes and the data they hold.

Privacy Rights

GDPR creates some new rights for individuals and strengthens some existing ones. The legislation provides the following: the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and rights relating to automated decision-making and profiling. In addition, the legislation introduces rights to protect children's privacy.

Data Security and Control

Data security and control are core requirements of GDPR. Article 5 entitled "Principles relating to processing of personal data" contains the bulk of the requirements. In essence, Article 5 says: data can only be processed for the reasons it was collected; must be accurate and kept up-to-date, and, if not, it should be erased; must be stored such that a subject is identifiable no longer than necessary; and must be processed securely.

Governance

GDPR includes provisions that promote accountability and governance. Organizations are expected to implement comprehensive governance measures that include the creation of a data protection officer position. Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

What Makes GDPR Different?

GDPR doesn't just expand the scope of legislation about data privacy; it also broadens the definition of the personal data that needs to be governed. It defines personal data as any information that can be used to identify an individual, directly or indirectly.

Personal data identifiers include: name; identification numbers; location data; and online identifiers. Also included are all factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a person.

GDPR applies wherever data is sent, processed or stored.

The Challenge for Organizations

The legislation will apply to thousands of organizations that didn't worry about EU data legislation in the past, forcing them to protect data that they didn't have to protect before. It also requires them to adopt a new attitude toward existing data. The days of harvesting information because it is easy and may be of value in the future are over. Even internal cross-department sharing of harvested personal data will require explicit consent.

Organizations' Data Security Obligations Under GDPR

Data Control

To preserve subjects' privacy, organizations must do the following:

- Only process data for authorized purposes
- Ensure data accuracy and integrity
- Minimize subject identities' exposure
- Implement data security measures

Data Security

Data security goes hand-in-hand with data control. GDPR puts security at the service of privacy. To preserve subjects' privacy, organizations must implement the following:

- Safeguards to keep data for additional processing
- Data protection measures, by default
- Security as a contractual requirement, based on risk assessment
- Encryption

Right to Erasure
Subject data cannot be kept indefinitely. GDPR requires organizations to completely erase data from all repositories when:

- Data subjects revoke their consent
- A partner organization requests data deletion
- A service or agreement comes to an end

The right to erasure has received a lot of media attention. It mandates that organizations need to fully erase a subject's data from all repositories when that person revokes his or her consent; when the purpose for which the data was collected is complete; or when compelled by the law.

However, it is worth noting that subjects do not have an unconditional right to be forgotten. If there are legitimate, legal reasons — as outlined in the regulation — an organization can retain and process a subject's data. However, exceptions are few compared to the many data uses common in our daily lives.

Risk Mitigation and Due Diligence
Organizations must assess the risks to privacy and security, and demonstrate that they're mitigating the risks.

They must:

- Conduct a full risk assessment
- Implement measures to ensure and demonstrate compliance
- Proactively help third-party customers and partners to comply
- Prove full data control

Breach Notification
When a security breach threatens the rights and privacy of a data subject or subjects, organizations need to notify customers and supervisory authorities.

They must:

- Notify authorities within 72 hours
- Describe the consequences of the breach
- Communicate the breach directly to all affected subjects

Fines

Depending on the violation, fines may range from 10 million euros to four percent of the total global profit, whichever is higher.

Supervisory authorities will base their fines on:

- The level of negligence involved
- Steps taken to mitigate damage and risk

Critical Need for a Project Plan

Before you jump into anything, find the GDPR legislation. Ensure you understand everything about collecting, processing, and storing data, and the legislation's many special categories, then create a road map for meeting the requirements. This starts with understanding the data you have, who has access to it, how and why it is shared, and what applications process data.

Begin with Critical Data and Procedures
Assess the risks to all private data, and review your policies and procedures. Apply security measures to production data containing core assets, and then extend those measures to back-ups and other repositories.

Here, you need to look at any risks to data not included in your previous assessments.

To support this effort, the (ISC)² EMEA Advisory Council GDPR Task Force has worked with the members' input they have been gathering to define 12 areas of activity and their key supporting tasks, along with for implementation. They are easy to understand, and communicate to the stakeholders who must be engaged to achieve them, and can be tackled simultaneously:

1. Stakeholder Support: Board and Business Units

Activities

- Identify seasoned professionals either from within the organization or externally (from your industry).
- Senior stakeholders who can support GDPR implementation need to be identified in each business unit/operation.
- Senior management must understand and champion GDPR requirements and the impact of non-compliance.
- Adequate resources such as budget and workforce need to be allocated.
- Responsibility for GDPR is required to be with the C-suite and executive management.
- Look for opportunity to create value with the exercise, review of processes; structuring of data, and so on.

Tip: Involve the people on the floor who are managing all the devices and ensure that your requests are specific for GDPR compliance.

2. Inventory of the Personal Information You Hold

Activities

- You may need to organize an information audit (a dataflow and a data inventory analysis), across the organization, or within particular business areas.
- The analysis should be matched with the consent given by the data subjects (put in a consent register) to verify, that consent is valid for the collection and operations (see action 7).

3. Privacy Notice and Information

Activities

- You should understand what must be communicated.
- Review your current privacy notices and put a plan in place for making any necessary changes.

4. Individuals' Rights

Activities

- Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
- Further national and international legislation may affect the rights of the data subject. For instance, accounting laws, logging directives, and so on may require the data to be stored beyond the requirements of GDPR.

Tip: Manually review exceptions in GDPR to make it workable and solve small issues. There will be gaps which will have to be explained to the Data Protection Authority (DPA).

5. Data Subjects' Access Requests

Activities

- You will need to update procedures, plan and document how requests will be handled within the new timescales and provide any additional information.

Tip: Security departments should delegate responsibility to operations and other parts of the organization.

6. Data Protection Impact Assessments (DPIA)

Activities

- You should work out how to implement DPIA in your organization. DPIAs can link to other organizational processes such as risk management and project management.
- You should start to assess the situations where it will be necessary to conduct a DPIA.
  - Who will do it?
  - Who else needs to be involved?
  - Will the process be run centrally or locally?

7. Consent

Activities

- You will need to review how your organization is seeking, obtaining and recording consent, and whether changes are needed.

Tip: Consider ways to collect data without the need for consent.

8. Children

Activities

- You should now start thinking about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9. Personal Data Breaches

Activities

- You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Tip: Tweak business continuity and security incident response plans that are currently in place.

10. Security of Data Processing and Data Protection by Design

Activities

- You should make sure you have the right procedures and tools in place to comply with both security and privacy by design requirements.

Tip: Companies following ISO 27001 compliance will have met much of the criteria.

11. Data Protection Governance

Activities

- You should designate a data protection officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements.

12. International Data Transfers

Activities

- If your organization operates internationally, you should determine which data protection supervisory authority you come under.
- Put simply, the lead authority is determined according to where your organization has its main administration or where decisions about data processing are made.
- In a traditional headquarters (branches model), this is easy to determine. It is more difficult for complex, multi-site companies where decisions about different processing activities are taken in different places.

Conclusion

The General Data Protection Regulation (GDPR) may look like an imposing and costly exercise, but the value for business and economies has the potential to be enormous for those who get it right. Companies today collect vast amounts of data. The GDPR compliance effort can be used to create opportunity by cleaning house, honing processes to collect the right information at the right time, and developing a stronger bond with the customers we collect it from. Simply put, it is an opportunity to take stock and make improvements.

Companies must begin by developing an understanding of what really matters to their business or organization. Any company that currently holds and works with personal data of EU citizens should be instructing every department to ask some basic questions about how and why they collect and use this personal data and the value it has to a given function or product line, before they consider what is needed to ensure they can continue to work with it. Such an approach will allow the development of a business case for the changes ahead and motivate the support required to devote the resources and budgets to enable the change.

Additional Resources

Looking for insight and help tackling GDPR compliance? Check out these other resources:

The (ISC)² Community GDPR Discussion Group

GDPR - Using Technology for Compliance

Prepping for May 2018 - A Guide to Complying with GDPR's Data Security Regs

GDPR - Now's the Time to Plan for Compliance

About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 130,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education™. For more information about (ISC)² visit www.isc2.org, follow us on Twitter or connect with us on Facebook.