WHITE PAPER

# GDPR: A Guidebook

Dataquest
Your Performance
is our priority

solarwinds
msp

## THE GENERAL DATA PROTECTION REGULATION GUIDEBOOK: MAKING SENSE OF A COMPLEX NEW LAW

*Understanding the new General Data Protection Regulation (GDPR) can be challenging. It's a complex law with confusing language. Making matters worse, the law has a far reach and prescribes potentially hefty fines for non-compliance. Without understanding the basics of the law, it could be easy to make an unwitting mistake that could cost you.*

For example, let's say you use an IT software vendor that suggests their products can help you achieve GDPR readiness. It's not necessarily bad to suggest that a vendor's products and services can help, but it's important to understand the facts around GDPR so you can distinguish fact from fiction. GDPR readiness is achieved by companies, not a single product. Organizations are ultimately responsible for their own GDPR compliance.

To help give you a clear understanding of key aspects of GDPR, we've put together the following guidebook. We'll cover the key terms, ideas on how to evaluate data breach impact, and even provide some pointers on how to move toward GDPR readiness. But first, we need to explain what GDPR is and who it impacts.

## A CRASH COURSE IN GDPR

What exactly is GDPR and what does it attempt to accomplish? In the time-honored tradition of the journalistic practice of answering the "5Ws and 1H," here is a high-level breakdown of GDPR.

### WHAT?

GDPR[1] is a regulation passed by the European Union (EU) that protects the personal data of EU citizens (also known as data subjects). GDPR defines personal data as any information relating to a data subject.

### WHO?

A data subject is defined as, "an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[2]." In short, a data subject is any EU citizen who has data about them collected by an organization.

### WHERE?

GDPR requires both the protection of personal data and evidence of the protection measures a business has in place for any location—physical or digital—where personal data is collected, processed, stored, or transmitted. Under GDPR, organizations must be able to identify when personal data becomes exposed or compromised.

The regulation applies to organizations regardless of whether they're located in the EU or not. To summarize Article 3 on Territorial Scope[3], GDPR applies to:

- Any organization in the EU, even if the processing occurs outside the EU
- An organization processing EU citizens' data in the context of selling goods or services or monitoring data subjects' behavior in the EU. This applies even if the organization is located outside of the EU
- Data controllers (defined as the entities that determine the purposes, conditions, and means of the processing of personal data ) that are located outside of the EU, but where the EU law applies due to international law

*GDPR was passed to respond to the rapid advancement of computer technology since 1995.*

## GDPR KEY TERMS

What follows is a series of terms found throughout the text of the GDPR. It's important to understand these terms, as they will be used in any GDPR-related correspondence, warnings, or other actions.

*On 25 May 2018, any enterprise located inside or outside of the EU that collect, process, store, or transmit personal data of EU data subjects must comply with the regulation.*

### DIRECTIVE

GDPR updates an older law called the Data Protection Directive. Lawmakers deliberately chose to make GDPR a regulation rather than a directive like the previous law. A **directive** sets a goal that every EU country must achieve via their own laws, but it does not dictate how the country must achieve the goal.

### REGULATION

A **regulation** must be applied as written across the entire EU. This distinction is important to understand, as an EU regulation will (in most cases) take precedence over an EU directive.

### DELEGATED ACTS

Considerable confusion may occur when a country's legislative act addresses an issue or situation that an EU regulation does not. Situations like these may result in delegated acts, which are, "non-legislative acts enacted in order to supplement existing legislation and provide criteria or clarity[5]."

### AUTHORITIES

When it comes to enforcement, each country has its own privacy and information office. These are collectively known as the GDPR Supervisory Authorities (SA), also known as Data Protection Authorities. SAs are, "national authorities tasked with the protection of data and privacy, as well as with monitoring and enforcing the data protection regulations within the EU[6]."

## ENTERPRISE

GDPR uses the word enterprise to describe any entity engaged in economic activity. The term applies regardless of the legal form of an organization including individuals, partnerships, and associations. This broad definition includes everything from sole proprietors to giant multinational corporations. This has serious implications—even small businesses and individuals must comply with GDPR rules, not just organizations with large IT budgets.

## DATA SUBJECT

A data subject is defined as, "a natural person whose personal data is processed by a controller or processor[7]." GDPR compliance is necessary to protect the personal data of data subjects. On 25 May, 2018, any enterprise located inside or outside of the EU that collect, process, store, or transmit personal data of EU data subjects must comply with the regulation.

GDPR further defines the data subject as a resident of the EU. Given the various categories of immigration visas, the word "resident" may need clarifying in the legislation. In some circumstances, such as a Canadian living in the EU, the protections of GDPR would be extended to that data subject's personal data. Regardless, it's important to realize that GDPR's protections extend the rights of EU residents outside the EU region.

## WHAT ARE SOME RIGHTS DATA SUBJECTS HAVE UNDER THE LAW?

In addition to other data subject rights, such as the right to be informed or the right to restrict processing, the **right to be forgotten**, also called the **right to erasure**, allows data subjects to demand that enterprises delete their personal data, stop transferring their data, and even keep third parties from processing their data. When receiving a request like this, businesses should confirm why data is being collected and whether it may be deleted, especially if there are other regulations requiring that such data not be permanently erased.

The **right to access**, also known as **subject access right**, allows the data subject to have access to any personal data held by an enterprise. If a subject requests access, the law requires enterprises to provide all personal data for the data subject.

Additionally, the data must be transferred to the subject in an electronic format. This part of GDPR refers to mandatory **data portability**. Data portability mandates that individuals have a right to receive their data in an easily accessible format. When providing personal data, an enterprise must redact the personal data of individuals other than the person requesting the data.

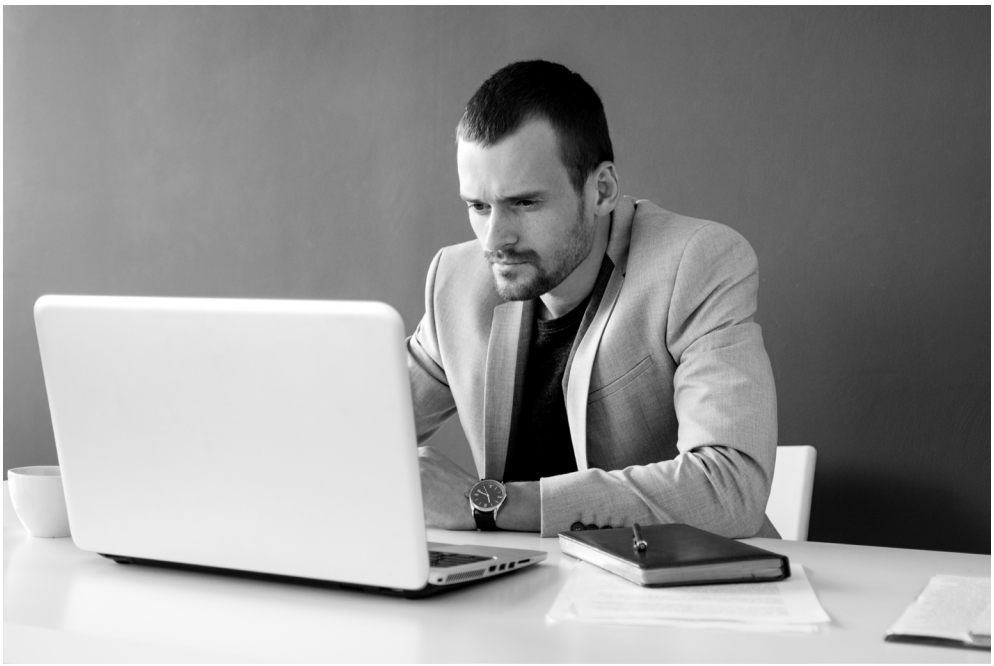
*The right to access allows the data subject to have access to any personal data held by an enterprise.*

## WHAT ARE SOME REQUIREMENTS PLACED ON ENTERPRISES?

If a business is going to rely upon the explicit consent to legally transfer personal data, the law requires that enterprises obtain **explicit consent** for the collection, processing, storage, and transmission of data subjects' personal data data. GDPR contains stringent requirements for consent. It must be freely given, specific, and informed. Additionally, GDPR requires that a data subject reviews a statement and signifies via explicit action their agreement to the collection, processing, storage or transmission of that subject's personal data.

Prior to GDPR, many countries had privacy legislation that differentiated the personal data protection responsibilities of a **data controller**—which is an enterprise that determines the purposes, conditions, and means of the processing of personal data—and a **data processor**—which is an enterprise that processes data on behalf of the data controller. Under GDPR, there is generally equal responsibility between data processors and controllers. Both controllers and processors share joint liability for personal data protection.

Some enterprises may be required to have a a **data protection officer** (DPO). A DPO reviews an enterprise's operations to build programs and processes to help an organization comply with its GDPR obligations. A key responsibility (and there are several) of the DPO is to conduct a **privacy impact assessment** (PIA) on various processing activities. During a PIA, the DPO will oversee an analysis of the personal data held by an enterprise as well as their security policies.



Another daunting challenge under GDPR is the **notification requirement**. In the event that a controller has a data breach, organizations should notify the SA and any impacted data subjects within 72 hours of discovering the breach. This part of the regulation can be confusing, as both "discovery" and "within 72 hours" could be open to interpretation.

*In the event that a controller has a data breach, organizations should notify the SA and any impacted data subjects within 72 hours of discovering the breach.*

For example, what constitutes "discovery?" Does this mean the business must monitor Twitter® 24/7 in case someone reports their personal data was breached? What happens if a routine security audit turns up indications of a data breach that happened months earlier? Many businesses will likely need some time to call in experts to confirm a data breach allegation by a third party. If you find yourself in this situation, we recommend consulting a legal expert on what responsibilities you'll have based on the new legal precedents.

Precisely when the SA and customers need to be notified (and by what method) is not expressly identified. It's fair to say a lot of press releases will declare, "the matter is under investigation and the relevant authorities have been apprised of the situation." But often, the evidence of a data breach may be difficult to obtain without expert Digital Forensic Incident Responders (DFIR).

When determining the severity and potential harm of a data breach, you need to take both the context of the data and the contents of the records into account. For example, there's a major difference in impact between a data breach that involves the title, surname, and first names for customers and one that involves complete tax documents or security clearance forms. However, regardless of the severity, the regulation does suggest that if a breach can cause the potential for harm, it should be reported.

## THE IMPORTANCE OF DATA PROTECTION AND MANAGEMENT

In the following section, we'll suggest some possible steps to take you closer to GDPR readiness. We want to emphasize that you should talk to a legal expert. However, these could be potentially important steps toward readiness for your business.

| NEXT STEPS |
| --- |
| 1. Create an internal roadmap |
| 2. Find and inventory all PII |
| 3. Map your data to facilitate data subject requests |
| 4. Map data processes |
| 5. Archive and encrypt or delete unnecessary data |

It may sound simplistic, but your first step should be to create an internal roadmap to figure out what you need to do for your customers. Once you figure what your organization needs to do to prepare for GDPR, then you can decide how you will inform your customers, employees, and suppliers of your intent.

One of your next steps involves personal data discovery—you cannot protect data that you don't know about. You must identify what data the business holds and why it holds that data. Under GDPR, you need to understand why you are processing the data, and if you are using explicit consent to process the data, data subjects need to consent to the use of their data. They must know why their data is being collected and how it will be protected. Taking an inventory of personal data will make it easier for you to truly protect users' personal data.

Another reason why you need to understand where personal data exists in your infrastructure is to facilitate data subject requests. Data subjects have the right to request access to their data, a copy of their data, that their data to be ported, and for their data to be erased.

Data management could become a nightmare for many businesses under GDPR. After years of operating, most business will have data, including personal data, located all over endpoints, servers, and even cloud services. The generic shared drive (S:\), with its ancient holiday party invites or payroll records from years ago, could be risky to retain without adequate protections.

You must examine and map business processes to understand the reasons data exists on your system. To help, use the questions in the following table to determine what data is collected, why it is collected, and whether the data is truly necessary. If you're uncertain, you may want to move the data to an archive or delete it entirely.

| WHAT IS THE CLASSIFICATION OF THE DATA? | WHO CREATED THE DATA? | WHERE IS THE DATA? | WHEN WAS THE DATA CREATED? | WHY IS THE DATA NECESSARY? | HOW WAS THE DATA CREATED? |
|---|---|---|---|---|---|
| Is it critical? | An employee? | Is it in one place? | Is it still necessary? | Regulation? | A production system? |
| Is it sensitive? | A system? | Is it in multiple places? | Does it still need to be "live?" | Historical? | An old system? |
| Is it regulated? | A customer? | Is it in the right place? | Has it been accessed recently? | Nostalgia? | Can it even be accessed anymore? |
| Is it needed by a third party? | Who knows? | Is it in a safe/ protected place? | Can it be archived? | No one knows | Can it be archived? |

There are quite a few questions you'll have to answer to truly understand a business's data landscape. But in short, the more data you have, especially personal data, the greater the risk of a data breach. It helps to reduce the amount of personal and non-personal data to make data protection and management easier.

Many legacy systems used by small and midsized businesses do not have adequate security controls. Some may transmit personal data in plain text or have known, unpatchable vulnerabilities (especially if the system isn't supported by the vendor anymore). With GDPR on the horizon, now's the time to consider hosted services for those legacy systems.

The systems that often contain a great deal of personal data are usually found in the Sales and Marketing, Accounting, and Payroll departments. If you find a hosted service that has robust security controls, you may want to consider migrating these legacy systems to the hosted services to take advantage of those enhanced security controls.

Once you identify personal data on your systems, you will want to assess how you are protecting it. Among other things, you may want to encrypt data at rest on mobile devices with BitLocker® on the Microsoft® Operating System, FileVault® on Apple® products, or by enabling the encryption option on Android® devices. Every EU member state is required to appoint an independent Supervisory Authority (SA). The job of the SA is to investigate complaints that relate to GDPR and approve administrative offences. An SA investigating a security incident under GDPR will look for evidence to suggest the business exercises due diligence (or not) when it comes to protecting the data subject's personal data. Documented proactive efforts on the part of the business become vital.

GDPR requires user security training for anyone using personal data. Providing user security training is potentially a quick win for a business's compliance efforts. These programs demonstrate a business's willingness to protect that data.

## GDPR AND DATA BREACHES

Whether it's from ransomware, a Trojan, or a lost device, data breaches can occur at any time. GDPR spells out specific rules on reporting these data breaches. As mentioned earlier, you must disclose a breach to the relevant authorities within 72 hours of its discovery. The notification you provide must, at a minimum, describe:

- The nature of the data breach
- The potential number of people and the approximate number of records that were affected
- The name and contact information of the point of contact from whom the supervisory authority can get more information
- The potential impact and consequences of the breach
- What steps the organization will take to remedy the situation and mitigate the damage

You can find more information on data breach notification requirements in article 33 of the GDPR text[8].

## DATA PROTECTION BY DESIGN AND DEFAULT

Article 25 of GDPR states that organizations must build in data privacy by design and default. In other words, best practices for data privacy should be followed on all projects. Article 25 roughly describes that:

1. When preparing for data processing and during the actual processing, an enterprise must apply appropriate technical and organizational safeguards to protect data.
2. The controller must implement technical and organizational safeguards to ensure that only the data required for a specific processing purpose is used. This includes how much data is collected, the extent of processing, and the retention period and accessibility of that data.

Additionally, organizations can apply for a certification of their compliance with this portion of the regulation. You can read more about certification in article 42 of the GDPR regulation[9].

### DATA PROTECTION IMPACT ASSESSMENTS

Another part of building data privacy into your processes is the use of data protection impact assessments. Article 35 of GDPR states that for any project that, "is likely to result in a high risk to the rights and freedoms of natural persons," a data controller must perform a data protection impact assessment[10].

According to article 35, the assessment must, at a minimum, contain:

- A description of the processing operations as well as a description of the purposes and legitimate interest of the controller
- An assessment of the degree and necessity of the processing operations
- An estimate of the potential risks to data subjects
- A statement about what safeguards you'll put in place to address the risks and comply with the regulation

For more information on requirements around data protection impact assessments, please read article 35 of the GDPR regulations[11].

## THE FUTURE AND GDPR

GDPR demands that the protection of personal data moves with EU data subjects no matter where their data is used. Because of this stipulation, there's a chance that GDPR will evolve into a global standard. The GDPR is set to arrive during a time when cybercrime is at an all-time high.

Europol's "Internet Organized Crime Threat Assessment" paints a bleak picture that indicates no letup in cybercriminal activity. From the report's executive summary:

*The 2017 Internet Organized Crime Threat Assessment (IOCTA) reports how cybercrime continues to grow and evolve. While many aspects of cybercrime are firmly established, other areas of cybercrime have witnessed a striking upsurge in activity, including attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions. A handful of cyber-attacks have caused wide-spread public concern but only represented a small sample of the wide array of cyber threats now faced*[12].

Data protection laws like GDPR will define data protection over the next several years. Compliance with GDPR is not optional, but hopefully, by providing greater data protection measures, businesses around the world will reduce the number of cybercriminal threats that affect both organizations and their customers.

1 GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

2 "Regulations," Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed October 2017).

3 GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

4 "The Impact of GDPR on Your Business," Osterman Research Blog. https://ostermanresearch.blog/2017/01/ (Accessed October 2017).

5 "GDPR Glossary," EUGDPR.ORG. http://www.eugdpr.org/glossary-of-terms.html (accessed October 2017).

6 "GDPR Glossary," EUGDPR.ORG. http://www.eugdpr.org/glossary-of-terms.html (accessed October 2017).

7 "GDPR Glossary," EUGDPR.ORG. http://www.eugdpr.org/glossary-of-terms.html (accessed October 2017).

8 GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

9 GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

10 GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

11 GDPR Final Text, Council of the European Union. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (accessed December 2017).

12 "Internet Organized Crime Assessment," Europol. https://www.thehaguesecuritydelta.com/media/com_hsd/report/152/document/iocta2017.pdf (accessed October 2017).

This document is provided for informational purposes only and should not be relied upon as legal advice or to determine how GDPR may apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance. SolarWinds MSP makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including the accuracy, completeness, or usefulness of any information.