What You Need to Know About GDPR

May 2018

Charles Lavallee, Vice President of Business Development

Venio Systems
Redefining Discovery

Executive Summary

With GDPR finally upon us, more and more articles are popping up each day on this complex topic. From insightful and expert opinions to the helpful quick-start guides, everyone is trying to make GDPR intelligible and prepare leaders for what is coming.

While some experts believe that no immediate impact may be felt, many remind all of us of the potential financial impact that sanctions will carry. We can all agree on the following: GDPR is going to change how organizations regard and manage personal and private data for all of us. Even those of us not living in the EU.

And at its core, an organization's success will teeter on the quality of preparation and well-defined (and documented) policies and processes. Below we offer a summary - not just what is to be expected from the employer, but also an overview of what people (aka in GDPR referred to as the 'natural person') should expect too.

If you are unfamiliar with GDPR, it is a new set of rules designed to give EU citizens more control over their personal data. GDPR stands for General Data Protection Regulations and is intended to bring privacy regulations into the 21st century. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.

Introduction

The European Union's General Data Privacy Regulations (GDPR) goes into force as law on May 25, 2018. These regulations provide consumers with important data protection and even though the GDPR began in the EU, it applies to any business or organization that offers services or goods to any EU resident. GDPR could become the defacto standard worldwide and noncompliance can carry penalties as high as 4% of annual global revenues.

Here are some of the key considerations for your organization looking ahead:

- US Companies may be more vulnerable than they think. With the increasing expansion of cloud and mobile computing, many US companies need to understand GDPR since they act as data processors and data controllers.
- Organizations that are third-party cloud providers could also be affected. Just because an organization relies on a third-party cloud provider to manage data, it does not mean they do not need to act.
- There are critical steps to take before and after GDPR goes into effect. GDPR is focused on ensuring that data protection laws are relevant and responsive given the increasing threat of security breaches and cyber-attacks. The goal is to help EU citizens feel safe when it comes to how they interact online.

We want to highlight three key ways GDPR will likely affect your organization and employees.

1. Your Organization's Responsibility to Create a GDPR Strategy

One critical first step is to identify who is accountable in your organization for assessing and developing a GDPR strategy. Some organizations call this a Data Protection Officer and this person should be well-versed in the data protection laws. The GDPR lead can work with the leadership team and communicate the regulatory requirements, monitor adherence, including performing audits and communicating and cooperating with the Information Commissioner's Office (the supervising authority in the EU).

Create Awareness of GDPR and Understand Its Implications for Your Company

Historically, "data subject" was the term used to describe a person; and with GDPR the term is now "natural person," which is a much broader definition of "personal data." GDPR will apply to consumer and business-to-business data as well. While the companies are not "natural persons", the individuals who work there are.

Here are a few first steps to keep in mind when creating a strategy and understanding where your organization is currently and where it needs to focus its efforts to be compliant with GDPR:

- Change happens from the top - ensure your leadership team understands why GDPR matters and the impact it will likely have.
- Identify which teams will be impacted the most - although communication should go out to the entire organization.
- Develop communication that goes to the teams that manage and process data, as well as your marketing teams that are capturing consent information.
- Review the personal data and information your company holds - do a privacy and information audit.
- Identify which companies you share data with and what information is shared.

Identify Your Current Procedures for Managing Personal Data & Privacy

Review your current privacy notices and ensure that your supporting procedures and processes support the changes necessary for GDPR.

- Review how you communicate privacy notices and develop a plan for making any necessary changes.
- Identify the process of deleting personal data as well as how you provide that data electronically and in a consistent format.
- Understand if your procedures are ready to handle requests from consumers to delete their information.

- Review your current documentation and ensure it shows how your organization is GDPR compliant. This includes existing contracts and arrangements you have in place when sharing data with other organizations.
- Make sure your privacy notice explains the lawful basis you have for processing the data as well as your data retention periods.

For the first time, processors will be held jointly liable for breaches, which requires compensation to individuals for damage caused by non-compliant processing.

Understand How Your Organization Will Handle Requests

According to Information Commissioner's Office, there are several key capabilities your GDPR process will need to be able to manage:

- Comply with requests within 30 days (currently, it is 40 days)
- In most cases, you cannot charge for complying with a request
- You can refuse a request if it is manifestly unfounded or excessive
- If you do refuse, you must be able to tell why and provide the information about the supervisory authority and a judicial remedy.
- This communication must happen within one month.

This process may require you to develop an online solution if you receive a lot of requests. Under GDPR, individuals will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

2. Understand the Individuals' Rights

It is important to know that your procedures cover all the rights of any individual. As we mentioned earlier, this should include how to delete personal data as well. GDPR includes the following rights for individuals:

- 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
- the right not to be subject to automated decision-making including profiling.

Some of the questions your organization should be able to answer include how to locate your data as well as how to delete the data and who makes those decisions.

What are the Special Categories of Personal Data?

Special categories of data have extra protection under GDPR. These will require explicit consent for processing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Genetic data (new)
- Biometric data (new)
- Data concerning health or sex life
- Sexual orientation

Any processing of personal data should be transparent to the natural persons that personal data concerning them are collected, used, consulted or processed and to what extent it will be processed. Any information that communicates how the data will be used must be: "easily accessible", "easy to understand", and "that clear and plain language" be used.

3. Review How You Will Seek, Record, and Manage Consent

Read the detailed guidance the ICO has published on consent under GDPR. There are multiple examples of what makes processing legal:

- It is necessary for the performance of the contract.
- It is in compliance with a legal obligation.
- It is necessary to protect vital interests of the data subject.
- It is in the public interest or exercising official authority.
- It is with the consent of the natural person.
- It is in the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the natural person.

In addition, it is important to understand what systems you may need to put in place to capture and verify an individual's age. You may need a parent or guardian's consent in order to process the information lawfully.

The consent must be specific, granular, clear, prominent, opt-in, properly documented, and easily withdrawn. (ICO)

What is Consent?

The definition of consent has new elements including the "unambiguous" indication of the subjects wishes and that a "statement or clear affirmative action" must be provided.

- "Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed."
- "Silence, pre-ticked boxes or inactivity should not, therefore, constitute consent."

In addition, the individual must know who they are providing their information to:

- the data subject should be aware at least of the identity of the controller and the intended purposes of the processing, (Recital 42);
- data subjects must be informed of their right to withdraw consent at any time prior to giving consent, (Article 7(3)); and
- to the specific information requirements found at Articles 12 to 14 of the GDPR that set out the information that must be given to the data subject to ensure fair and transparent processing.

"Consent is one lawful basis for processing, and explicit consent can also legitimize use of special category data. Consent may also be relevant where the individual has exercised their right to restriction, and explicit consent can legitimize automated decision-making and overseas transfers of data." ICO

Here is an excellent checklist for Consent from the ICO.

Review and Assess the User's Experience

These changes will no doubt affect how your client or customer engages with your organization and the ease at which they provide consent and are informed about who has access to their data.

Utilize this opportunity to build trust with your customers and show transparency while making the process easy to understand and use. Many companies keep the disclosures long and cumbersome. Simplifying the language of your communications and providing transparency to your customers is a great way to engage and protect your reputation.

Please reach out to us if you have additional comments or questions. Email us at info@veniosystems.com with feedback or suggestions.

About the Author: Charles Lavallée

The 18-year eDiscovery veteran joined the company's growing team as Vice President of Business Development in 2017. His responsibilities include helping organizations evaluate their solutions, workflows, and processes and partnering with them to leverage Venio's unified platform for better decision making, greater efficiency, and cost savings.

About Venio Systems

At Venio Systems, we are dedicated to working with our trusted partners to bring the latest legal technology innovations to law firms, agencies, and corporations. We provide e-Discovery solutions that streamline and improve the litigation process for our clients and partners, allowing them to achieve the most successful outcome possible while saving time and resources.

Experience the VenioOne difference with our unified platform that powers every phase of e-Discovery: processing, early case assessment, legal analysis, culling, review, and digital production. Our VenioOne OnDemand self-service solution provides users an agile and easy to use system throughout the litigation process.

Bring all phases of e-Discovery from processing through production under one platform with VenioOne.

References

Information Commissioner's Office. Consultation: GDPR consent guidance Available at: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Information Commissioner's Office. ICO Checklist for Consent. Available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Information Commissioner's Office. Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now. Available at: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Gillett, P. A Marketer's Guide to GDPR. Available at: https://medium.com/ama-marketing-news/a-marketers-guide-to-gdpr-91cdb0940554