General Data Protection Regulation (GDPR)

Understanding its impact on your organization and how Church Office Online's products will be compliant.

Church Office Online

Understanding the GDPR and its **impact on your organization.**

Table of contents

GDPR Overview

What Is It?

The GDPR is legislation passed by the European Union (EU) Parliament, focusing on the protection of the personal data of EU residents. The legislation is unique as it sets forth regulations for any business which controls or processes EU resident data, regardless of the organization's location. It grants individuals greater control over their personal information, giving them a say about how their data is handled, including what information is used, whether it is transferred to third parties, and when it is erased.

The GDPR regulation also enhances the definition of "Personal Data," adding several criteria. This is important, because while the new regulation is specific and only pertains to personal data, the scope of what is considered personal has expanded.

> "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one 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. – Art. 4(1)

When does GDPR go into effect?

May 25, 2018

Who does the GDPR affect?

In order to properly address who the GDPR affects, we must define a couple of key terms, namely "Data Controller" and "Data Processor." (Referred to here as "Controller" and "Processor.")

If you are interested in learning more, the full legislation and additional regulation details are here.

These two subjects are the most directly impacted by requirements set forth by the new regulation.

Controller

The term "Controller" has particular importance under the GDPR, as compliance obligations under EU data protection law are primarily imposed on Controllers. It is important to note that while Controllers bear the primary responsibility for compliance, Processors also have specific obligations.

"Controller" means the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. – Art. 4(7)

Processor

GDPR defines the term "Processor" as any entity which processes personal data on behalf of the Controller or by instruction of the Controller. Many service providers fit within the definition of a Processor. Processing ranges from collection and storage to transfer and manipulation of data.

"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. – Art. 4(8)

Not only do all organizations working within the EU Member States fall under the authority of the regulation, but any organization, EU-based or not, which processes personal data of or offers goods and services to EU residents. If your organization has employees, members, prospects or customers who are EU residents, you are required to meet GDPR compliance standards. Much of the regulation is similar to the EU Data Protection Directive of 1995, which the GDPR replaces. Arguably the greatest differences between the two are the GDPR places more control in the hands of the consumer, and more responsibility for security and privacy compliance on the Processor.

What are the consequences of failing to comply with the GDPR?

For compliance infractions, the GDPR supervisory authority is empowered to fine businesses "20 million Euros or up to 4 percent of total worldwide annual turnover in the preceding financial year," whichever is greater.

Regulation Basics

Though they are not the only areas of compliance detailed within the GDPR, there are several key principles from the regulation to note.

Transparency

The EU Data Protection Directive of 1995 currently requires data is lawfully and fairly processed. However, the GDPR brings forth an additional requirement: Transparency. Simply stated, Controllers and Processors are required to fully disclose how and why data is processed, and they must disclose that information to data subjects in clear and simple terms. Privacy Policies and Terms and Conditions documents will no longer be written in cryptic legalese and hidden in hard to find places. They must be both easy to access and easy to understand.

Consent

Per the GDPR, consent must be "freely given, specific, informed and unambiguous," and is one of several reasons Processors and Controllers may use to justify the processing of data.

Additionally, the regulation requires that—especially when consent is related to sensitive data—it must be "explicit," meaning the user is knowingly and actively granting consent to process said data.

Pre-checked boxes, therefore, are not considered consent—users must actively check the consent box themselves. Along the same lines is the right to revoke consent; for consent to be considered "freely given," the data subject must have the ability to withdraw consent at any time.

Sensitive data is considered any data whereby "the context of their processing could create significant risks to the fundamental rights and freedoms" of the data subject, and is further defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

There are some additional protections for acquiring consent to capture and process the data of a minor. The definition of a minor has been left to the individual Member States. Some States define minors as children under the age of 13, while others set the age at 16 and under. The GDPR requires consent for a minor is captured from the child's legal parent or guardian. The Controller is then tasked with making "reasonable efforts" to validate the identity of the parent or guardian before processing data. When a minor's data is captured and

Privacy policy documents will no longer be written in **cryptic legalese** and hidden in **hard to find places**.

processed (with valid consent of a parent/guardian), the individual is granted the right to request his or her data no longer be processed, or deleted outright, once they reach majority. The GDPR recognizes individuals may not have understood the impacts of processing their data as a minor, and should have the right to revoke consent once they become an adult.

Right to be forgotten

Data subjects have the right to erase their data, and the Controller and Processor must comply when requested to do so. However, there are caveats. For example, if the Processor still has the legal obligation to hold on to the data (i.e., bookkeeping law requiring purchase data to be stored for a period of time until transactions finalize), they are not obligated to delete it. But, the data must be deleted upon request when any of the following apply, as defined by the GDPR:

- The data is no longer needed in relation to the purposes for which the data was collected or processed;
- The data subject withdraws consent;
- The data subject objects to the processing of personal data concerning them;
- The processing was performed unlawfully.

The act of erasing the personal data of a subject is complicated for Processors and Controllers. They are obligated to map every bit of personal data associated with an individual and wipe it out when requested. It should be noted that cryptographically erasing the data is a potential solution. This is the process of encrypting data based on a key and then the key is deleted, preventing the encryption from ever being reversed.

Security and privacy program management

One of the more interesting principles of the GDPR regulation is the need for Processors to implement a Privacy Program, which potentially includes the appointment of a Data Protection Officer (DPO). This is often an executive level individual, but can also be comprised of a team of security and compliance professionals. The DPO oversees the security and privacy strategies instituted within an organization.

Some of the objectives the DPO is responsible for includes: Defining and maintaining processes to ensure the protection of user data, conducting internal privacy audits, informing Controllers and data subjects of their rights and responsibilities, and handling inquiries or complaints related to GDPR compliance.

The GDPR is clear in its distinction that the DPO is intended to act as an advocate for the regulation, Controllers and data subjects. It goes so far as to dictate the role reports only to the executive level, have and maintain its own budget, and follow strict conditions for dismissal, with the final say residing with the Data Protection Authority (DPA)—an independent supervisory authority for the regulation.

The regulation also requires organizations perform Data Privacy Impact Analysis (DPIA) when processing proposals introduce a high level of risk to data subjects. For example, if a new feature includes processing sensitive personal data or large-scale processing, the company must perform a DPIA prior to project initiation. A DPIA is intended to help identify and avoid or reduce the potential risks to personal data.

Privacy policy updates are made to clearly define the data captured and the **rights of our users.**

The use of pseudonymizing in general processing is also recommended by the GDPR. As defined in the regulation, this is 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."

Basically, identifying markers are replaced with random values, or pseudonyms. This results in the ability to use the data without openly identifying the associated individual. The pseudonymized data is traced back to its originating source. While it offers some protection from, for example, profiling, it does not fully protect the data subject if the information is hacked.

Data breach protocol

When personal data is accessed without authorization, it is the responsibility of the Processor to notify the Controller, who must then notify the DPA within 72 hours of identifying the breach. Details about what data and how it was stolen must be included in notifications, as well as the plan or steps taken to correct the breach, and potential consequences to data subjects impacted.

Limitation of purpose and collection

Simply put, the GDPR states only data with a true business purpose and transparently disclosed to data subjects should be collected and processed. Data subjects must be clear on what you collect, why you want it, and how you use it—with that as the basis behind the collection.

Businesses cannot state "we want it for market research." They must prove a legal basis for processing, show it is in the organization's "legitimate interest," or garner explicit consent from the data subject to use it for that purpose.

Data Protection by Design

The Data Protection by Design principle requires organizations to have security and protection protocols in place, and to have security and data protection as a foundation for all future development. This goes hand in hand with performing a DPIA for high-risk processing activities, but also demands organizations ingrain data-protection principles into any developments.

When designing new features or functions, make sure to minimize the amount of data processed to only what is absolutely necessary, ensure it is fully protected, and delete it when it's no longer used. The GDPR asks businesses to integrate data protection into their development culture.

Compliance for products at Church Office Online

At Church Office Online, we take compliance and data protection seriously. We are dedicated to closely working with our partners, customers and Controllers to ensure we meet our obligations as a Processor and data protection advocate. We partner with an industry leading privacy and compliance expert to analyze our business processes and applications, and to assist us in determining where we need to make changes. As a result of this evaluation, we are making adjustments to become compliant.

The additional compliance steps we and each of our brands are taking to meet GDPR standards include:

Document updates

- Updating our data privacy and legal documentation to ensure we are transparent with our processing and providing our Controllers with the details they need to have clear, informed insight into what we do with customer data. This includes ensuring our documentation is easy to understand, detailed and consistent across all of our brands.
- Updating our security program documentation to better expose how we protect the data we process.
- Updating our contracts to further clarify the privacy and security responsibilities of each party involved in the agreement.

Process updates

Updating our processes to provide assistance to our data Controllers when they have an obligation to respond to an individual's exercise of rights.

Feature design

Updating our security and design protocols to fully integrate the "data protection by design" principle.

Training

Training our support, implementation and account management teams to help guide our clients and partners in their compliance efforts. For example, our implementation teams will be encouraging our clients to provide GDPR-complaint Privacy Policies to end users and assist them in setting up their applications.

Functional changes

Making functional changes to some areas of our product applications to better provide our customers with the tools they need to be compliant. The changes differ from product to product. Several of our brands already provide tools to meet compliance, and will only release minor additions.

Unequivocally, Church Office Online believes in the goals of the GDPR, and the regulations it is designed to enforce. We also hold closely to the idea we are partners with our customers, providing them data security and protection of personal data.