prezentor.
CLEVER SELLING

General Data Protection Regulation

What it is, what we are doing, and what you can do

Disclaimer: Please note that this guide is for informational purposes only, and should not be relied upon as legal advice. We encourage you to work with legal and other professional counsel to determine precisely how the GDPR might apply to your

BACKGROUND

Since 1995 data protection has been enshrined in the European Union privacy directive (95/46/EC). As of May 25, 2018 this directive will be replaced by the new General Data Protection Regulation (also known as the GDPR) which will have a range of significant implications for organizations as well as individuals.
In essence the GDPR is an attempt to harmonize, strengthen and update EU data protection law to ensure that the legislation follows the technical advances. Special emphasis is placed on enhancing individual rights and freedoms, aligned with the basic principle of privacy as a fundamental human right.
It is important to note that there will not be a 'grace period' for compliance with the GDPR, wherefore it is important for the organizations impacted to get ready for it now.

WHO WILL BE AFFECTED?

Fundamentally the scope of the GDPR is very broad;

The GDPR will cover:

1. all organizations established within the EU, and;
2. all organizations involved in processing the personal data of EU citizens.

Being that the GDPR will cover any and all organizations processing the personal data of EU citizens (also known as the principle of extraterritoriality), it will have the implication that the GDPR could apply to any organization anywhere in the world (across all sectors), regardless of it's main place of establishment and the location of their processing activities.

Therefore it is vital for companies to perform an analysis of whether they are processing personal data on EU citizens.
To aid your understanding of the expansion of scope outlined in the GDPR a description of a few definitions are necessary;

WHAT IS CONSIDERED ‘PERSONAL DATA’?

As per the GDPR, personal data is defined as any information relating to an identified or identifiable individual, whereby information that could be used on its own or in combination with other available data to identify an individual is covered. Thus the scope of the definition of personal data is extremely broad and could potentially cover a wide variety of data.

Under this definition not merely data commonly deemed as personal in nature will be included (e.g. names, physical addressees, email adresses), but in addition also data such as IP-adresses, behavioral data, location data, financial data, and much more. Hence for Prezentor customers, at least a majority of the data you collect on contacts will fall within the definition of personal data.
One should also be aware that even personal data which has been rendered immediately un-referable to an individual (pseudonymized) can be considered personal data if it is possible to link the data to the individual by auxiliary means.

Sensitive personal data, such as information related to health, will require greater measures of protection. This data may be stored in the Prezentor platform, however you will need to follow the special guidelines in order to protect the data concerned.

HOW IS ‘DATA PROCESSING’ DEFINED?

As defined in the GDPR’s article 4, (2):
’processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

In other words, if you are collecting, managing, using or storing any personal data of EU citizens, you are processing personal data within the definition outlined by the GDPR.

Even if you do not believe your business activities to be covered by the GDPR, you may still want to consider the GDPR and the underlying principles, as European law tends to set the legislative course for further development. Additionally as consumers are becoming increasingly aware of privacy in the virtual domain, you may gain a competitive edge by complying with privacy principles now rather than later.

CHANGES IN OBLIGATIONS DUE TO GDPR

While the underlying principles and rationale of the Directive remain the basis of the GDPR, several important and ambitious changes are introduced.
We have highlighted the following points as we believe them to be of particular relevance to Prezentor as well as our customers:

1. **Expansion of scope**
   As described previously, the territorial scope is expanded with the introduction of the GDPR - all organizations established or processing data of EU citizens will be covered, which effectively extends the scope well beyond the borders of just the EU.

2. **Expansion of definitions of personal and sensitive data**
   As outlined above, the GDPR widens the definitory boundaries for what is considered personal data. This is a crucial change as it may be conceptually challenging to grasp exactly what is covered by the term, personal data.

3. **Expansion of individual rights**

- Right to be forgotten: An individual may request that an organization delete all data on that individual without undue delay.

- Right to object: An individual may prohibit certain data uses.

- Right to rectification: Individuals may request that incomplete data be completed or that incorrect data be corrected.

- Right of access: Individuals have the right to know what data about them is being processed and how.

- Right of portability: Individuals may request that personal data held by one organization be transported to another.

4. **Stricter consent requirements**
   Consent is one of the cornerstones of the GDPR, and organizations must therefore ensure that consent is obtained in compliance with the GDPR's stringent new requirements. You will need to obtain consent from your contacts for every specific usage of their personal data, unless you can rely on a separate legal basis, such as those found in number 5 below. However the safest route will be to obtain explicit consent, which is why we have developed GDPR-friendly forms to facilitate obtaining consent.

   Things to consider with regards to consent:

   - Consent must be specific and informed to distinct purposes.
   - Silence, pre-ticked boxes or inactivity does not constitute consent; data subjects must explicitly opt-in to the storage, use and management of their personal data.
   - Separate consent must be obtained for different processing activities, which means you must be clear about how the data will be used when you obtain consent.

5. **Stricter processing requirements**
   Individuals have the right to receive "fair and transparent" information about the processing of their personal data, including:

- Contact details for the data controller.
- Purpose of the data: This should be as specific (“purpose limitation”) and minimized (“data minimization”) as possible. You should carefully consider what data you are collecting and why. Ultimately you shall be able to validate the aforementioned to a regulator.
- Retention period: This should be as short as possible (“storage limitation”), of course with due respect to other valid reasons for retention, such as legal/ regulatory requirements or professional guidelines.
- Legal basis: You cannot process personal data merely because you want to. You must have a valid “legal basis” for doing so, such as where the processing is necessary to the performance of a contract, an individual has consented, or the processing is in the organization’s "legitimate interest.”

As there are many other principles and requirements introduced by the GDPR that may apply to you, it is vital to review the GDPR in its entirety to ensure that you have a complete understanding of all its requirements and ultimately ensure compliance.

ENSURING YOUR COMPLIANCE WITH THE GDPR

In order to gain an overview of the full scope of your compliance obligations, you should consult with legal and other professional counsel. Generally speaking, however as noted above, *if you are an organization that is organized in the EU or one that is processing the personal data of EU citizens, the GDPR will apply to you*. Even if all that you are doing is collecting or storing email addresses, if those email addresses belong to EU citizens, the GDPR will *likely* apply to you.

CONSEQUENCES OF NON-COMPLIANCE

One of the key reasons for the intense focus on the introduction of the GDPR are the potential enormous financial penalties. Sanctions for non-compliance can amount to 20 Million Euros or 4% of global annual turnover, whichever is higher.

ROLE DELEGATION - CONTROLLER / PROCESSOR

In the context of accessing, processing etc. personal data, the requirements and obligations will depend on whether you act as either a controller or a processor. Under the GDPR, a controller determines the purposes and means of processing personal data, as well as the specific personal data that is collected from a contact for the processing.
As such the GDPR has not fundamentally changed the definitory frame, but is has however expanded the responsibilities of the respective parties.

Controllers will retain primary responsibility for data protection (including, for example, the obligation to report data breaches to data protection authorities, the obligation to fulfill contacts rights etc.); the GDPR additionally places direct responsibilities on the processor.

In the context of the Prezentor platform, in the majority of circumstances, our customers are acting as the controller. Our customers, for example, decide what information from their contacts is entered into the Prezentor platform; with or without the purpose to send emails to those contacts.
Prezentor is acting as a processor by performing these and other services for our customers.

PREZENTOR'S COMPLIANCE WITH THE GDPR

Since the inception of Prezentor, safety has been a focus, which helped constitute a basis for the new data privacy efforts, we have initiated. At Prezentor, we believe the GDPR represents a global trend of enhanced focus on the importance of data privacy in a world increasingly dominated by Big Data. We view the maintenance of sufficient security and privacy structures as instrumental to any SaaS' company's successful operation, and are thus committed to achieving compliance with the GDPR by May 25, 2018.

Prezentor's GDPR preparation started a year ago, and as part of this process we are reviewing (and updating where necessary) all of our internal processes, procedures, data systems, and documentation to ensure that we are ready when

the GDPR goes into effect. While much of our preparation is happening behind the scenes, we are also working on a number of initiatives that will be visible to our users. We are, among other things:

- Implementing full encryption of database
- Implementing novel functionality to enable customers to obtain GDPR-compliant consent
- Updating our Data Processing Agreement to meet the requirements of the GDPR in order for Prezentor to continue to lawfully receive and process that data;
- Updating our third-party supplier contracts to meet the requirements of the GDPR in order to permit us to continue to lawfully transfer EU personal data to those third parties and permit those third parties to continue to lawfully receive and process that data;
- Analyzing all of our current features and templates to determine whether any improvements or additions can be made to make them more efficient for those users subject to the GDPR;

PREZENTOR'S ASSISTANCE IN YOUR GDPR COMPLIANCE EFFORTS

With the GDPR implementation deadline hastily approaching you should start your compliance efforts now, if you haven't already. It is never too early to review your organization's data privacy and security practices, and there are several ways in which Prezentor can help.

Expansion of Individual Rights
Prezentor can help you respond quickly to requests from your contacts pursuant to their expanded individual rights under the GDPR.

Right to be forgotten: You may delete individual contacts upon their request at any time.

Right to rectification: You may access and update your contacts lists within your Prezentor account to correct or complete contacts' information upon their request at any time.

Right of access: You may generate a report of data related to individual contacts upon their request at any time.

Right of portability: You may export a report of data related to individual contacts upon their request at any time.

If you have specific questions about the GDPR and your use of Prezentor, you can email support@prezentor.com.