GDPR Strategy

Dated: 23/03/2018

Introduction:

GDPR stands for General Data Protection Regulation—a major piece of legislation passed by the European Union (EU) that could significantly impact your business whether your organization is based in the EU or not. With fines up to 20 million or 4% of global revenue for violating GDPR, it's a piece of legislation that no one can afford to ignore.

GDPR is an opportunity to build a stronger data protection foundation for the benefit of all. Fondesk is committed to ensuring that our platform is GDPR-compliant when the regulation becomes enforceable on May 25, 2018.

What is Data Processing, who are Data Subjects, and What is Personal Data?

GDPR is all about protecting the rights of data subjects in connection with processing their personal data.

Data Processing

Data processing is really just anything you can do with or to data. It includes accessing it, collecting it, reading it, storing it, analysing it, retrieving it, organizing it, transferring it, disclosing it, and deleting it.

Data Subjects

Under GDPR, data subjects are just people — human beings.

Personal Data

Personal data is data that relates to “identified” or “identifiable” data subjects. An “identifiable” data subject is someone who can be identified, directly or indirectly, such as by reference to an identifier like a name, ID number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Note how broad the definition of personal data is. It can include data such as the IP address of an individual’s personal device, a device ID, or phone number. It doesn’t matter that the identifier could change (e.g., that the user could change their phone number or device ID).

GDPR defines certain categories of personal data as extra sensitive. These special categories are personal data revealing race, ethnicity, political opinion, religious or philosophical beliefs, trade union membership, and also genetic data, biometric data, health data, or data concerning the data subjects’ sex life or sexual orientation.

The rule under GDPR is that these types of data should not be processed unless a special exception applies such as the data subject providing explicit consent, or the processing being necessary to protect the life of the data subject and the data subject is incapable of giving consent. In addition to special categories of personal data, GDPR also has special rules for processing children’s data (data of data subjects under age 16) and data relating to criminal convictions or offenses.

Data Controllers and Data Processors

GDPR carries over the concepts of data controllers and data processors from the Directive. Similar to the Directive, data controllers and data processors have different obligations under GDPR. Therefore, it’s important to understand whether you’re acting as a data controller or a data processor in relation to the various categories of personal data you process.

WHO IS A DATA CONTROLLER?

GDPR defines a data controller as “the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data.” In other words, if your organization processes personal data for your own organization’s purposes and needs—not

merely as a service provider acting on behalf of another organization—then you are likely to be a data controller.

WHO IS A DATA PROCESSOR?

Businesses or organizations that process personal data solely on behalf of, and as directed by, data controllers are data processors. In other words, when a data controller outsources a data processing function to another entity, that other entity is generally a data processor.

DATA SUBJECTS' RIGHTS

As a corollary to the above principles, data subjects have certain rights regarding their personal data. In fact, GDPR puts the onus on controllers to facilitate the exercise of these rights (see Article 12). Controllers must only use processors that can reasonably ensure protection of these rights, and processors, for their part, are expected to reasonably assist controllers in responding to data subjects' requests to exercise their rights (see Article 28).

1. **The right to be informed**

   Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

   Read More >>

2. **The right of access**

   Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

   Read More >>

3. **The right to rectification**

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- You have one calendar month to respond to a request.
- In certain circumstances you can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

Read More >>

4. The right to erasure

- The GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

Read More >>

5. The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, you are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21). Read More >>

6. The right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.

Read More >>

✓ Fondesk allows you to export your call, message, reports and other logs into a commonly used format.

7. The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Read More >>

8. Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process. Read More >>

Data Processing Obligations

Now that you understand who data subjects are, what personal data is, and whether you are a controller or processor of that personal data, let's discuss what are you supposed to do (or not do) with data subjects' personal data under GDPR.

OUR GDPR OBLIGATIONS

Fondesk understands that the focus on individual rights (as well as transparency and accountability for the collection and handling of personal data) places EU residents and their rights at the heart of GDPR. Therefore, we will ensure that our organization makes all the necessary changes in order to support the GDPR regulations. These include the 8 rights as mentioned above. As such, we will consider all aspects of data processing activities, storage and disposal of all personal data.

In addition, we accept that the new regulations strengthen compliance requirements including new rules on consent and clear definition of how data is to be used. We will adopt a Privacy by Design ethos and complete Impact Assessments (where necessary) to understand how best to guarantee data is kept secure.

We also accept the need for transparency, including Breach Disclosure Requirements to notify authorities and in some cases, data subjects within 72 hours.

Our strategy is based on the following key principles:

We will be a responsible custodian of customer and employee data. The Customer and Fondesk acknowledge that the Customer is the Controller and Fondesk is the Processor in respect of any Personal Data supplied to Fondesk by or on behalf of Customer, including Personal Data in the course of the supply of the Data Processing Services.

The Data Processing Agreement applies to any Processing of Personal Data performed by the Processor in connection with the performance of the Data Processing Services to the Controller.

We will assign clear ownership for data privacy across the company starting at the highest levels, with clear responsibility and accountability for all aspects of data security throughout the organization.

Fondesk

- We will establish a formal inventory of data processing operations and supporting systems that collect, process and store personal data.
- We will review and verify the legal basis for collecting and processing personal data; as well as the legal means for any cross-border (outside Europe) transfers and communicate this clearly with all data subjects.
- We will regularly review all systems and processes, identify gaps and develop a plan to achieve compliance within the new regulations.
- We will review partners and vendors to establish current contract terms and agreed upon data protection controls.
- We will ensure we can support individuals exercising their rights under the GDPR.
- Fondesk fully supports the requirements of the GDPR and will ensure appropriate resources and funding are available to meet these obligations in preparation for 25 May 2018 implementation.
- We are adopting a risk managed approach and acknowledge that there may be gaps in implementation. However, we will have completed high priority tasks, review and made significant changes in order to support the GDPR.
- We offer various tools that you can use to make your account more secure or the resources in your account more secure.

- Additionally, all access to customer data is protected by roles and permissions within the Fondesk system. Fondesk employees can only access data on a need-to-know basis, and according to “the principle of least privilege,” which means Fondesk employees have the minimal level of access to data in order to do their job.
- When we process and access data, it’s always with consent— whether it’s in accordance with our Data Processing Agreement or with explicit customer consent. That ensures we fulfil our legal obligation to our customers to protect their data at all times.
- Additionally, we require that each department document any process that relates to the processing of personal data. To protect our system against internal abuse, we also ensure Fondesk employees are given the minimum access to data required to carry out their role.

- Customers that want to delete communications content from Fondesk’s systems, such as voice recordings or message bodies, can make use of the DELETE functionality.
- We use SSL (Secure Sockets Layer), the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

- Fondesk leverages AWS data centers for all production systems and customer data. AWS follows industry best practices and complies with an impressive array of standards.

For more information on AWS Data Center Physical Security, see the AWS Security Whitepaper:

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

We will make sure to do the following:

- only collect information that is needed for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as needed, and only for as long as need it; and
- allow the subject of the information to see it on request.

Please see our full terms and privacy policies for details.

GDPR Strategy Document. Registered in England.