WHITEPAPER

Is your business ready for GDPR?

By 42Gears Team

Table of Contents

The General Data Protection Regulation (GDPR) will be the top priority for any business dealing with EU subject's private information. Each member state in EU operates as per the 1995 data protection directive, which is going to be replaced by new GDPR. EU aims to provide individuals more control on their personal data and in order to control the free movement of this data, it must replace the old directive. The GDPR law will be applicable to all EU member states and the UK as well. Businesses have been granted two years' time to make them GDPR compliant. Organizations dealing with data of the residents of the European Union will have to comply with the GDPR rules. Non-compliance will result in severe fine charges levied upon them.

This paper will help businesses to understand the GDPR, its principles, penalties and essential steps to be taken while executing GDPR.

Introduction

The Data Protection Laws in the European Union (EU) have been going through several changes since the last two decades. The EU has decided to enforce new laws to improve data protection for individuals. With new regime, EU aims to provide individuals more control over their personal data accessed by EU enterprises. These enterprise have been riding the wave of digital revolution and the old directives will no longer be sufficient to protect customer data. GDPR was adopted in 2016 and is considered to be the biggest change in the old regime. It will be applicable from May 25, 2018 onwards.

Organizations should be well aware of the consequences as non-compliance with GDPR laws could lead to strict penalties. GDPR rules have been designed to enable businesses to streamline and standardize operations and ensure that their products and solutions comply with the defined guidelines.

This paper attempts to help businesses understand how GDPR will work and making them aware of the harsh consequences of non-compliance with the new law. It offers an analysis of how GDPR will bring consistency in business models and standardize the operations. It will also help individuals ascertain data privacy rules while embracing technological innovations.

GDPR Insights

For years, Information Technology and digital business models have revolutionized the business world and changed lives significantly. The digital world has introduced many contemporary data privacy challenges posed by newer technologies such as social media, Internet, mobile apps, and behavioral marketing. These challenges were at their early stage of manifestation when the previous directive was designed. Over time, the old rules have fallen short of the requirement to safeguard customer data. Now, EU has decided to introduce a new law-GDPR that addresses all the challenges that its predecessor has failed to address. Though, the new GDPR data protection law will replace the data protection directive of 1995, it will still largely retain the main principles while also adding new features such as strict rule of consent, data portability requirement and a right to be forgotten. Unlike the old directive, GDPR does not require governments to pass any enabling legislation, and is directly binding and applicable.

Many multinational companies responsible for handling personal information of individuals will also embrace GDPR to bring more consistency in work and reduce the cost of dealing with multiple data protection authorities. However, they should be aware of the bigger changes that the new law will bring in, as well as its pros and cons.

Who will be impacted by GDPR?

The GDPR applies to all organizations that offer goods or services to, or monitor the behavior of EU data subjects, whether they are located within or outside the EU.

Entities affected by GDPR

- Companies located within EU
- Companies located outside EU but process personal data of EU residents.
- Entities working with more than 250 employees
- Entities working with less than 250 employees but their data processing impacts the rights and freedom of data subjects

The data formats covered under GDPR are audio, video, photographs, IP address and device IDs. The definition of personal data is also explained here which is quite important to understand.

Personal data: Any data which is used to identify an individual, either directly or indirectly, or as part of a collection of data spread across multiple systems. It also includes genetic, biometric, social, political, cultural, economic and mental information.

Now, the important point to consider here is whether an entity or organization is controller or processor. The article 4 of EU GDPR has defined these two terms as under:

Controller: "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."

Controller organization is the 'extracter' of personal data. And is the primary responsible for the

Processor: "A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

For example, organizations (controller) stores customer data in a CRM system (processor) and a marketing system.

How to prepare businesses for GDPR

GDPR will have varying effects on businesses depending upon the extent to which they are extracting or managing personal data of EU subjects. Some will be affected more than others. However, they need to analyze the quantum of affect and how they should prepare for it. *According to PwC GDPR Preparedness Pulse Survey, 54% said that GDPR is their top data protection priority.*

Data protection is at the heart of GDPR. Businesses should strategize around it as GDPR is expected to cause big impact.

According to an Ovum survey, in order to accommodate new data privacy law, 2/3 of businesses have to change their global business strategies. Also, to accommodate the law, businesses are expecting a 70% rise in their business budget.

To get ready for GDPR, businesses need to understand the GDPR guidelines/principles, the GDPR penalties in case of breach of law and the essential steps to be taken before enforcement of law.

How to prepare businesses for GDPR*

As per Article 5 of GDPR, the principles related to processing of personal data are explained below:

Lawfulness, fairness and transparency

Principle.1:

- Information should be provided by controller to data subject about personal data processing.
- Before collecting data, the individual should be informed.
- A mandatory list of information should be given to individuals on when data is obtained directly or indirectly.

Purpose limitation

Principle.2:

- Processing personal data is permissible only to the extent it is compliant with the original purpose.
- Processing for another purpose requires further consent.

Data minimization

Principle.3:

- Data must be adequate, relevant and limited to purposes for which they are processed.
- Controllers must ensure that only required data is being accessed and not more than that.

Accuracy

Principle.4:

- Personal data should be kept accurately and up to date.

Storage limitation

Principle.5:

- Personal data should be deleted once the purpose is fulfilled.
- Regular review process should be conducted with methodical cleansing of database.

Integrity and confidentiality

Principle.6:

- Personal data should be protected against unauthorized access.
- Controllers and processors should assess risk and implement appropriate security measures to protect breaches.

Accountability

Principle.7:

- Data controllers must be able to demonstrate compliance with other principles.
- Controllers shall be responsible for non-compliance.

The above mentioned principles should be followed while accessing and processing EU subject's data. Non-compliance will subject companies to harsh consequences and huge penalties, which may vary from country to country. More details are given below:

GDPR Penalties

GDPR empowers regulators to penalize businesses that does not comply with its guidelines. In case any business is found to be involved in data breaches, improper data processing and don't have data protection officer, they can be penalized. There will be two levels of penalties under GDPR.

The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher. For more details refer here.

Essential steps to be taken

Organizations, in order to be compliant with GDPR, are required to go through the following essential steps or checklist. Businesses need to assess which part of their organization is going to be impacted the most and the crucial steps that needs to be taken.

- **Awareness among key people**

All the key people and decision makers should be well aware of the changes the new law is going to make. Moreover, they should appreciate the impact GDPR is likely to have and identify those areas that can cause compliance problems. Large organizations should be extra cautious while implementing GDPR as it will involve significant resource changes.

- **Maintaining records processing details**

An organization, in order to comply with GDPR, requires documenting all the details regarding what information it holds, from where it was extracted and with whom these details are going to be shared.

- **Ensuring procedures cover individual's rights**

Organizations should check if they are following procedures that are fulfilling individual rights such as the right to be informed, right to object, right to access, right to data portability, right to rectification, right not to be subject to automated decision making, and right to restrict processing.

- **Processing lawfully**

Companies should identify the lawful basis to process personal data under GDPR. They should document how they will do it, conduct review from time to time and update the processes.

- **Plan consent issues as per GDPR laws**

In GDPR, to seek, record and manage consent are very important and require timely revision and updates. The consent as per GDPR standard should be specific, clear, prominent, granular, opt-in, well documented and flexible to be withdrawn. If the company fails to fulfill standards, the consent mechanism should be changed and refreshed.

- **Considering age factor**

If an organization engages in processing personal data of children and relies on their consent to collect information, the company is required to have permission from the child's parents or guardians. As per GDPR laws, the child must have attained the age of 16 to provide consent or before this age companies must seek consent from their parents.

- **Preparing for the data breaches**

An organization must plan or document the procedures for data breaches. It is the duty of companies to report to Information commissioner's office (ICO) on any data breaches that involve any damage to an individual's reputation, financial loss, loss of confidentiality or any sort of economic and social loss.

- **Data Protection Impacts Assessment (DPIA)**

A DPIA is required in some situations where data processing involves high risk to individuals such as deployment of new technology, significant effect on individuals due to profiling operations, and the case where special categories of data are being processed on large scale.

- **Data Protection Officers (DPO)**

It is quite important to have someone who can take the responsibility of data protection compliance and have proper knowledge of the matter. It is mandatory to have DPO if it is a public authority, or an organization that carries out regular data monitoring of individuals, and those organizations that are involved in data monitoring of special categories such as criminal convictions or health records of individuals on large basis.

- **International**

Organizations working internationally or with more than one EU state need to take utmost care of data protection laws. They should determine the data protection supervisory authority and are required to document laws properly.2

GDPR Readiness Checklist

- Do you know what data in your organization contains personal data, including unstructured sources such as documents?
- Do you know how you use or process personal data and for what purpose?
- Do you know what consent was given (or later retracted) for which purposes, for this personal data?
- Do you know what security controls are in place for personal data, and whether this data is deleted or anonymized appropriately once the consented usage has finalized?
- Can you respond to regulatory requests about the usage and storage of personal data, in the timeframes required by the GDPR?
- Can you scale your ability to respond to potentially thousands of concurrent requests (e.g., as part of a class action lawsuit)?
- Do you store personal data in multiple languages?
- Are you treating personal data as a valuable asset to enhance customer experience and potentially develop new products?

Conclusion

The GDPR will have a big impact on businesses in EU member states and across the world. EU envisioned the negative impact of growing Information Technology on individual's data privacy, resulting in the conceptualization of a new GDPR law.

It will provide many benefits such as boosting business's reputation in the eyes of potential customers, a much high level of consumer and client trust due to greater data security, cybersecurity will improve and more.

To comply with GDPR, businesses will be required to change their strategies, models, products and solutions.

42Gears takes utmost care in protecting customer data. The processes and products are designed to ensure data privacy. We periodically perform audits and checks for compliance. 42Gears products help customers in their GDPR compliance endeavor.

Reference:

1. https://united-kingdom.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html

2. https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf