ACQUIRE

GDPR

A Phenomenal change to The Data Protection Industry

www.acquire.io

Introduction

The General Data Protection Regulation 2016/679 (GDPR) replaces the old 1995 Data Protection Directive 95/46/EC, setting a new bar for privacy rights, security, and compliance around the world. GDPR regulates the processing of personal data belonging to people living in any of the EU member states (Data Subjects). The GDPR, a pivotal change in the history of data privacy regulations, affects each and every organization worldwide that collects, stores, and processes data on persons in the EU. The GDPR will replace legal complexity with a single, unified law. On May 25, 2018, the existing Data Protection Directive, and the laws relating to it, will no longer apply. Fines for non-compliance with the standards can reach up to 4 percent of the organization's global turnover, or up to 20 million Euros, whichever is higher.

This whitepaper serves as an introduction to the GDPR and will help you accelerate your response it by providing a basic understanding of what is contained within different sections of the regulation.

Background

An individual's personal data is used today by both public and private organizations to carry out their activities on a large scale, and we still have no idea how our personal data travels through unprotected platforms and devices. We easily trust the organization handling our data and assume that they have adopted standards to manage personal data and process, collect, or share our details in a way that we find acceptable to do so. But sadly, this is not the case. A considerable number of organizations still lack the procedures to ensure data security. The latest research shows that the number of data breaches has significantly increased over the years. This highlights the need to strengthen enforcement measures and enact resilient legislation to face the data protection challenges that we experience today. The GDPR will be used as a starting point to build a consistent environment dedicated to the protection of individual personal data.

Need for the GDPR

The Data Protection Directive was established in 1995, which was over twenty years ago, when internet connectivity required a dial-up connection and mobile phones were not that smart. The dramatic change in technology and the way data has been collected, processed, and used since then have compelled a change to the outdated data protection laws. The expansion of the internet, mobile processing devices, and superfast broadband connections have created a boom in the way we share, store, and process personal data. The GDPR is more of a regulation than a directive, and will significantly change the way personal data and data breaches are handled, and leverage the rights of individuals residing in the EU. The intention behind the reformation of this data protection regulation is to strengthen and reinforce individuals' rights through clear and robust rules for free movement of data, thus, setting a consistent and global data protection standard.

Scope of the GDPR

The scope of the GDPR is broad, but the basic principles on which it stands focus on the processing of data, either automated or not. In general, anyone who processes personal data of EU citizens, whether they are data controllers or data processors, in the EU or not, is subject to the GDPR.

Key Principles of the GDPR

The EU's GDPR provides a clear overview for dealing with security and protection of personal data. But organizations are still confused on what to enforce and how to handle the security of their data in accordance with this regulation. The path to compliance with the GDPR will be different for every organization, but the key principles will provide a more comprehensible view.

1. Lawful, fair, and transparent processing

According to the first principle of the law, the data processing handled by the organization must be transaparent and fair to the data subjects, and must meet the laws described in the GDPR.

2. Purpose limitation

This principle suggests that the organization needs to have "specified, explicit, and legitimate purposes," which the subject has been made aware of, and no other without further consent.

3. Data minimization

Based on this principle, the organization must ensure that the data they capture is adequate, relevant, and limited, i.e. only storing the minimum amount of data required for their purpose.

4. Accurate

The requirement of this principle is that the data controllers must ensure that the data or information remains accurate and valid to the purpose for which it was gathered. This ensures the protection of data against identity theft.

5. Storage Limitations

This principle suggests that personal data should not be retained unnecessarily, and thus, kept in a form that permits identification of data subjects for no longer than necessary.

6. Confidential and Secure

This principle requires processors to handle data by implementing appropriate security measures that are proportionate to the risks and rights of individual subjects. Achieving compliance to these principles requires the organization to evaluate their security policies, handling access control and authentication procedures, and protecting them against malware/ransomware attacks.

Moving forward

Although the key principles of data privacy from the previous directive still hold true, many changes have been proposed to regulatory policies. Here are the major points of the GDPR and its impacts on organizations.

Territorial Influence

The new regulation has no boundary restrictions when it comes to handling EU citizens' personal data. Whether you are in the US or India, if you are dealing with the data of EU citizens, you must comply with the law. There are other regulations that cross geographic boundaries; for example, ISO 27001 and PCI DSS; but they are more specific to organizations and are handled in a simplistic manner. The GDPR is more complicated and wide-ranging, and it applies to the processing of personal data of individuals in the EU, irrespective of whether the processing takes place in the EU or not.

Entities of the GDPR

There are different roles defined under the GDPR to formalize the regulation across organizations in regards to their responsibilities.

1. Data Processor

A processor is reponsible for processing personal data on behalf of a controller. They are either service providers or outsourced vendors, and their responsibilities can also include storing data in the cloud. As a processor, they need to maintain records of personal data and processing activities.

2. Data Controller

Controllers determine the “purposes and means of processing the personal data.” They have a direct responsibility to the data subject and to the data protection authority. The data controller is also liable to ensure that the data processors are GDPR compliant.

3. Data Subjects

Any individual belonging to the EU whose personal data is processed by a controller or processor.

4. Data Protection Officer

A security expert who must operate independently to oversee data security strategy and compliance in an organization, as dictated by the GDPR. Under the regulation, the appointment of a DPO is mandatory if the controller and processor are involved in the core activities of personal data processing operations.

Scope of Personal Data

The definition of personal data, which has widened in scope under the regulation, is any information that relates to an identified or identifiable living individual. The GDPR also defines “special categories” of personal data, which have additional restrictions and requirements (data regarding religion, biometrics, ethnicity, race, etc.). Personal data can include name, surname, email address, identification card number, location data, IP address, cookies, etc. In particular, this pertains to any data or information that is somehow linked and tracked back to an individual, even if it is de-identified, encrypted, or pseudonymized; it is still considered personal data.

Accountability

Accountability places a burden on the data controller to demonstrate compliance by developing and maintaining appropriate and sufficient internal records. In addition to this, complying with the regulation is not enough, and thus, the controller will have to keep records justifying individuals’ consent, and may have to prove this to the European Regulator. Privacy Impact Assessments must be in place to review data processing activities.

Data Breach Notifications

A data breach is an incident that involves unauthorized or illegal access or sharing of information. Most data breaches occurs due to unauthorized intrusions and hacking attempts. An organization under the GDPR may be required to update their breach reporting procedures, as the regulation requires that an organization must report certain types of data breaches to the relevant supervisory authority (the Information Commisioner’s Office in the UK) within 72 hours. Notifications must include the nature, identity, recommended measures to prevent adverse effects, and process for addressing the breach.

Security and Privacy by Design

To secure the personal data of individuals, controllers and processors may need to identify security protocols that are in place and update them, as part of the legal requirement of the GDPR. Privacy by design is an important concept and requires that data protection be considered at the intial stage of any project, and requires that the system be configured and designed to be inherently secure. Security and privacy by design must be explicitly considered according to the GDPR, applying strict security and privacy controls at all times, and requiring permitted access and functionality for each process. Controllers and processors must demonstrate compliance by applying the following controls:

1. Encryption, anonymization, and pseudonymization of personal data must be taken into account by the organization to lower risk.

2. The organization must ensure that the confidentiality, integrity, availability, and resilience of systems are maintained while processing.

3. Ensure that only authorized persons can access personal data by implementing the appropriate access controls.

4. For infrastructure security, ongoing monitoring and detection procedures must be in place.

5. To prevent data loss in the event of a failure or disaster, processes must be adopted to deal with such incidents.

Right of Data Subject

The GDPR leverages data subjects' privacy by providing exclusive rights in the handling of their personal data. However, these rights can be a headache for controllers and processors, as they face practical problems in identifying and retrieving relevant data assets in order to process them. Data subjects' rights under the existing Data Protection Act will still be protected under the new regulation. However, they are strengthened and extended to include three more key rights:

1. The Right to erasure

The data subject has the right to be erased or forgotten, and can withdraw their consent if it is found that their data was processed unlawfully or they have any legal reason to be removed. The change must be handled appropriately by the operator.

2. The Right to object to processing

Data subjects have the right to object to the processing of their personal data according to their consent, where consent is the legal basis of processing.

3. The Right to data portability

This means that data subjects are, at any time, allowed to receive their personal data in a commonly used format. Under this right, individuals can ask one company to share personal data with another.

Consent and Transparency

Organizations will have to redefine the consents that were previously obtained, as the new regulation has strict consent requirements and non-compliance is unlawful. Controllers and processors will now have to provide consent in a clear and specific way. In addition to this, consent must be different for each processing activity, with no pre-checked boxes, and must be transparent to data subjects. To be transparent in processing activities, organizations must notify and provide an opt-out option for data subjects. Privacy policies should be updated to include where the data is sent or processed, who is responsible for its storage, how long it is being stored, how it is intended to be used, and whether it will be transferring outside of the EU. Furthermore, the ability to withdraw consent must also be easily obtainable.

Data Processing

Under the GDPR, you need to identify the “legal basis” for processing, as you cannot process personal data without good reason. Organizations must specify why the processing is Under the GDPR, you need to identify the “legal basis” for processing, as you cannot process personal data without good reason. Organizations must specify why the processing is necessary, whether data subjects have consented to the processing of their data, and if the processing is in the organization’s legitimate interests. Controllers and processors must identify themselves and their responsibilities, thus, agreeing to their respective privacy obligations to avoid repudiation.

International Data Transfers

Organizations are prohibited from transferring data outside the EU unless they have a certain number of safeguards. Transferring data to a third country can only be possible if that country has been determined by the EU Commission to have an adequate level of protection by decision. For US-based companies, it is important to self-certify under the EU/US Privacy Shield. Standard Contractual Clauses or Binding Corporate Rules are related safeguards adopted by multinational companies to make inter-company personal data transfers.

Conclusion

The most recent surveys have indicated that while the deadline is only two weeks away, only 7% of businesses are GDPR-ready. Many organizations have not yet realized that not complying with the GDPR can seriously impact their business. They need to understand that the GDPR is not as simple as data security; it goes beyond that. Organizations must adapt their data protection procedures. However, maintaining a comprehensive data inventory, secure storage, appropriate access controls, and encryption can be the first step in demonstrating compliance.

Detailed guidelines and information on GDPR can be found at these two websites:

The EUGDPR website: www.eugdpr.org

The Information Commissioner's Office (ICO) Website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/