NOVEMBER 1, 2022

GDPR: INTRODUCTION & SERVICES

WHITE PAPER BY AUUDITR

Introduction

Data protection and privacy are major concerns today, where businesses are growing daily and reaching out to global markets. European Union has taken an enormous step by passing data protection regulations in 2018 and making these regulations obligatory for EU-based organizations. The General Data Protection Regulations (GDPR) is now the fastest-growing Act to get compliance to run businesses. GDPR considers consumer data an asset that should be managed and protected responsibly. In failing to do so, GDPR is permitted to penalize companies and face grave consequences. The primary purpose of passing this law was to protect European citizens and standardize the data protection laws under the umbrella of GDPR. This act ensures that organizations consider data protection while conducting their business.

GDPR thoroughly deals with data security, data privacy, and data transfer to third parties while keeping it protected and maintaining the data, considering the type of supervision required. GDPR allows organizations to use different standards as frameworks for implementation or regulation.

This paper discusses the main content of GDPR, its implementation methodology, and Auuditr's way of working and approach.

"European Union has taken a huge step by passing data protection regulations in 2018 and made these regulations obligatory for EU based organizations."

Keywords: GDPR, Data Protection, Europe, Auuditr, Cyber Security, Subject Rights, GDPR Penalties, European Union, Data Protect Act

Context

European Union took the considerable step to pass a regulatory act when people rely on cloud services for their data. Other services where organizations use personal or sensitive information also needed guidance on what to consider while protecting the data. Security breaches have become widespread in a world where data is the most potent tool. GDPR is regarded as the most strict security and privacy law that not only imposes the regulations as an obligation but also levies harsh fines and penalties if the data privacy standards are violated.

GDPR is a general guideline for the management of data. It is flexible enough to use other security standards like ISO 27001 to implement data privacy laws. It's a law that empowers citizens to have the power of their data moved among service providers or get their data erased.

The structure of GDPR consists of 11 chapters and 91 articles. These articles provide guidelines about:

- Rights of data subjects
- Responsibilities of data controllers
- Data protection impact assessments
- Maintaining security while recording, processing, and storing the data
- Data breaches
- Remedies of the breaches
- Penalties in case of breaches
- Rights to the public data or processing of data related to sensitive communities

The regulatory acts and their details are further discussed in upcoming sections of this paper. Furthermore, this paper also discusses the type of organizations that can go for compliance with GDPR and Auuditr's services offered to their clients.

Who can comply with GDPR?

GDPR is a law that makes it an obligation to follow for European businesses. Other organizations working globally and need to target markets in EU regions must get complied with GDPR to win the trust of their clients.

It is not only an obligation but an effective way to achieve Cyber Security and data protection and reduce the risks of data breaches. Companies already certified in ISO 27001, ISO 29100 or NIST can quickly achieve compliance, as GDPR guidelines also cover aspects of data security from these standards.

GDPR applies to the following:

- Organizations or some parts of them work with data processing.
- All types of businesses, i.e. software houses, internet service providers, cloud services, enterprises depending upon public data from Europe, some parts of manufacturing and service industries where the citizen data might be involved and more.
- Companies need to win the trust of their clients and get on top of their competitors.

"Companies that are already certified in ISO 27001, ISO 29100 or NIST can easily achieve compliance."

Structure of the Regulations

The structure of the regulations is divided into 11 chapters and 91 related articles. The chapters' context is as follows:

1. **Chapter 1 (Art. 1 – 4)**
   This chapter sets the basic understanding of the upcoming rules. It tells about the subject matter and objectives, definitions of terms used, and material and territorial scope.

2. **Chapter 2 (Art. 5 – 11)**
   This chapter's objective is to explain data processing principles. Lawfulness, consent, and processing of special categories of data are discussed.

3. **Chapter 3 (Art. 12 – 23)**
   The rights of data subjects are discussed in detail here. Transport of information, rights to access the data subject, rectification, erasure, processing, data portability and restrictions are the main contents.

4. **Chapter 4 (Art. 24 – 43)**
   The purpose of this chapter is to define the roles of data controller and processor. The responsibilities and the extent to which they can work with the data are discussed.

5. **Chapter 5 (Art. 44 – 50)**
   Chapter 5 discusses data transfer to international organizations and explains the safeguards that must be applied to protect the data.

6. **Chapter 6 (Art. 51-59)**
   This chapter discusses the supervisory authorities and their roles. The competency level of supervisor authorities, rules they must follow, powers they possess and tasks they must perform.

7. **Chapter 7 (Art. 60 – 76)**
   This chapter explains the duties performed by the supervisory authorities to maintain consistency while monitoring the conformity of the law. It also describes the working of the data protection board and its constituents.

8. **Chapter 8 (Art. 77 – 84)**
   This chapter discusses the penalties and rights of data subjects in case of data breaches.

9. **Chapter 9 (Art. 85 – 91)**
   These are the general guidelines about specific situations and data processing in some instances. Also, this chapter discusses safeguarding public data, processing data for research, etc.

10. **Chapter 10 (Art. 92 – 93)**
    This chapter discusses the details of delegated authorities in the articles discussed in the previous chapters.

11. **Chapter 11 (Art. 94 – 99)**
    This chapter is generally about the revisions in the regulations as mentioned earlier or other introduced provisions.

Services Offered by Auuditr

As a consultancy firm, we offer our team the expertise to develop processes and management methods to ensure organizational information security. We provide the following services:

- Gap assessment sessions to find out the existing capability of the organization
- Policies and procedure guidelines
- Data protection guidelines
- Incident management guidelines
- Consultancy sessions
- Tools & templates

Though GDPR seems simple and easy to follow, in practice, it is complicated to implement in practice. Auuditr is here to help you in detail with the complex development and implementation of the standard. Our team is well equipped to understand the detail your organization chooses to go into the standard and makes the standard into implementable portions of processes that can be followed.

Further information on

www.Auuditr.com