VOLUME 24, MAY 2021 ISSN 2456-9704

UNDERSTANDING GDPR: THE BRAINCHILD OF THE EUROPEAN UNION

By Aishwarya Gowda
From Ramaiah College of Law

Introduction:

Acting as the toughest privacy and security law, the GDPR came into force on 25th May 2018, although it was enacted 5 years ago. Passed by the European Union, the GDPR imposes liability upon any organization that collects data related to the people in the European Union. Every organisation associated with collecting data from the citizens of the EU comes under the purview of this Act.

GDPR holds the organisations accountable and imposes harsh fines upon them. This applies to anyone violating the standards of security and privacy set forth.

The General Data Protection Regulation offers the citizens of the European Union rights via rules set forth, which lets them control their personal data effectively.

The main aim of the GDPR is to simplify the digital economy in the European Union to benefit its citizens.

The GDPR enhances how people can access information. This information can be used by any organisation. The GDPR protects the citizens by setting forth certain limitations on the organisations and sets rules regarding the usage of this information.

History of GDPR- Exploring the predeceasing directive of 1995:

The General Data Protective Regulation was adopted in April 2016 replacing the previously existing and outdated directive of 1995. The pre-existing directive was more flexible and allowed the members of its states to adopt and implement rules accordingly. They were empowered to customise it according to the needs of their citizens. The new regulation firmly dictates that all the members of the state must adopt the regulation wholly and comply with the same. The timeline given below lays down the important dates and events from The Data Protection Directive of 1995 up to the birth of The GDPR, 2018.

24th October,1995: The European Data Protection Directive on the protection of people concerning the processing of personal data and on the free movement of the data was adopted.

22nd June, 2011: An opinion was put forth by The European Data Protection Supervisor.

25th January, 2012: A comprehensive reform was proposed by the European Commission in regards to the 1995 Directive. It suggested the strengthening of online privacy rights and boost the digital economy of Europe.

7th March,2012: An opinion on the commission's data protection reform package was adopted by the European Data Protection Supervisor.

23rd March, 2012: An opinion on the data protection reform proposal was adopted by the Article 29 Working Party (WP29).

5th October, 2012: Further input on the data protection reforms discussion was provided by the article 29 working party.

12th March, 2014: The European Parliament displayed support with a total of 621 votes in favour, 10 against and 22 abstentions.

15th June,2015: The previously existing Article 29 will be replaced by the European Protection Data Board. This board shall ensure the consistency of the application of the GDPR throughout the union, through guidelines, decisions and opinions.

27th July, 2015: The European Data Protection Supervisor published recommendations to European co-legislators negotiating on the final text of the GDPR in the form of suggestions. A mobile app comparing the commission's proposal with the parliamentary text was launched.

15th December, 2015: An agreement was reached on the GDPR by the Council and the Commission.

2nd February, 2016: An action plan for the implementation of GDPR was issued by the Working Party 29.

27th April, 2016: Regulation (EU) 2016/679 of the EU Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of private data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

24th May, 2016: The Regulation came into force 20 days after its publication in the official journal of The European Union.

10th January, 2017: Two new regulations on the privacy and electronic communications and the data protection rules were proposed by the European Commission. This applied to European Institutions.

6th May, 2018: Members States must have transposed the Data Protection Directive for the police and justice sectors into national legislation. it'll be applicable from 6th May, 2018.

22nd May, 2018: Proposal for a Regulation of the European Parliament and the Council was passed. This regulation associate with the protection of individuals concerning the processing of data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation

25th May, 2018: Corrigendum to Regulation (EU) 2016/679 of the EU Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of private data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) was issued.

25th May, 2018: The General Data Protection Directive deemed to be applicable from this day forward.

Objectives and Purpose:

After a comprehensive discussion spanning over the course of 4 years, the GDPR, The brainchild of the European Union replaced the previously existing Data Protection Directive of 1995. Adopted by both the European Parliament and European Council in 2016, the regulation holds its place as the world's strongest set of data protection rules. Article 1 of the GDPR lays down the objectives and purpose. It states the following:

1. This Regulation lays down rules relating to the protection of natural persons concerning the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons concerning the processing of personal data.[1]

The fundamental purpose of passing this regulation was to protect natural persons and their rights. Article 8(1) of The Charter of Fundamental Rights of The European Union and Article 16(1) of The Treaty on The Functioning of The European Union provides that everyone has the right to protection of personal data concerning him/her. [2] The fundamental rights and freedom should be respected while processing any personal data and this personal data must be protected.

This regulation focuses on the strengthening of the economies and contributes to an area of freedom, security and justice, resulting in economic and social progress within the International and internal markets.

Rapid technological developments and globalisation have brought new challenges for the protection of private data. the dimensions of accumulation and sharing of private data has increased significantly. Technology allows both private companies and public authorities to create use of private data on an unprecedented scale to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and may further facilitate the free flow of private data within the Union and the transfer to 3rd countries and international organisations while ensuring a high level of protection of private data.

Those developments require a robust and more coherent data protection framework within the Union, backed by strong enforcement, given the importance of fabricating the trust which will allow the digital economy to develop across the market. Natural persons should have control of their data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for creating the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

To create a uniform level of protection for natural persons throughout the Union and to avoid divergences hampering the free movement of private data within the market, a Regulation is critical to ensure legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to bestow natural persons in the Member States with an equivalent level of legally enforceable rights and obligations and responsibilities for controllers and processors, to adhere consistent monitoring of the processing of

[1] www.gdpr-text.com

[2] www.privacyregulation.eu.org

private data, and equivalent sanctions in the Member States as well as effective cooperation between the supervisory authorities of various Member States. appropriate functioning of the market requires that the free movement of private data within the Union isn't restricted or prohibited for reasons connected with the protection of natural persons concerning the processing of private data.

The purpose of the GDPR is to impose a consistent data security law on all EU members, so each member state no longer writes its own data protection laws and laws are consistent across the whole EU. Additionally to EU members, it's important to notice that any company that markets goods or services to EU residents, despite its location, is subject to the regulation. As a result, GDPR will have an effect on data protection requirements globally.

Personal data under GDPR:

According to Article 4(1) of the legislation, *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*[3]

To summarise this article, the term personal data includes:

- Name
- Address
- Photos
- IP address
- Genetic data
- Biometric data
- Location data
- Political opinion
- Sexual orientation
- Racial or ethnic data

Principles set forth by the legislation:

The GDPR in Article 5 sets out of 7 key principles. They are:

- Lawfulness, fairness and transparency: Data shall be lawfully processed in a fair and transparent manner.
- Purpose Limitation: Data shall be collected for specified, explicit and legitimate purpose only.
- Data minimisation: Data collected shall be adequate, relevant and limited to what is necessary.
- Accuracy: Any inaccurate personal data collected shall be erased or rectified without any delay.
- Storage limitation: Data shall not be stored for longer periods after being processed.
- Integrity and Confidentiality: Integrity and confidentiality is to be maintained while collecting and processing data.

Types of companies affected by GDPR:

Any company that stores or processes personal information about EU citizens within the EU states must befit the GDPR, albeit there is no business presence in the EU. Criteria required by the companies are:

- Company must be present in the EU
- Any data processed from the EU residents

[3] www.gdpr-text.com

- Company accommodates more than 250 employees.
- Companies with less than 250 employees but the data processed impacts the rights and freedom of the data subjects and include sensitive personal information.

Non-Compliance and Penalty:

The regulation specifies standards for data protection and electronic privacy within the European Economic Area, and also the rights of European citizens to regulate the processing and distribution of personally-identifiable information.

Your organisation must follow the principles stated within the Regulation and keep appropriate documentation that proves you're following those rules.

You must also perform regular risk assessments to see if your circumstances have changed, in which case you'll ought to update your data processing processes and documentation accordingly.

Violators of GDPR could be fined up to €20 million, or up to 4% of the annual worldwide turnover of the preceding fiscal year , whichever is larger.

To avoid these penalties, a company in order to comply with the GDPR must

- Update its privacy policy
- Prove compliance through a comprehensive framework
- Establish accountability and proper governance
- Brief the employees on the benefits and risks of GDPR
- Audit current data
- Develop necessary policies to cover compliance
- Obtain consent from every consumer and understand its importance
- Constant security checks to audit data processing
- Maintain and update company records
- Apply Data Protection Impact Assessment when necessary

Here are some of the biggest GDPR fines imposed to date:

- British Airways – 204.6m Euros
- Marriot International Hotels – 110.3m Euros
- Google Inc. – 50m Euros
- Austrian Post – 18.5m Euros
- Deutsche Wohnen SE – 14.5m Euros
- 1&1 Telecom GmbH – 9.5m Euros

To conclude, The GDPR was created to adapt to the new age of internet whilst creating a strict sense of liability. When the '95 Directive was drafted, the landscape of technology was divergent. With the growth of internet, social media, and the general sharing of data across the globe, a strict law to protect one's personal data was the need of the hour. Therefore, GDPR was drafted keeping in mind the technological advance and the protection of one's identity and information.

*****