VOLUME 20 ISSN 2456-9704

GENERAL DATA PROTECTION REGULATION (GDPR): AN ANALYSIS

By Sakshi Singh
From Adv balasaheb Apte College of Law, Mumbai

ABSTRACT
The General Data Protection Regulation (GDPR), which is a set of rules and regulations aimed to give European citizens more power over their personal data and information is unquestionably the most significant change in the European Union's data privacy regulation. This regulation replaced the obsolete Data Protection Directive (DPD) 95/46/EC which was introduced in 1995. The EU's GDPR came into effect on May 25, 2018, and the main purpose of this regulation is to regulate the immense incursion of personal information being processed by entities around the world. The GDPR, consists of 173 recitals and these recitals cover forty-five detailed rules on data processing, forty-three conditions of applicability, thirty-five bureaucratic requirements for EU member states, and seventeen totaled rights and aims to protect the fundamental right to data protection. As stated by the European Commission, the most significant purpose of this legislation is to provide the data subjects, additional control over their personal data and to make business. This Article addresses, the most vital parts and matters of this regulation, its influence on individuals and businesses as well as an assessment of its results and actual impact.

INTRODUCTION
In this new electronic age "privacy" is a major concern. Even the best data security systems cannot protect our private information from getting leaked. "Personal information" is any information relating to us, it can be about our professional or private life and reveals a lot about us and our thoughts. While data can be used for valuable purposes, the unrestricted and arbitrary use of data, specifically personal data has raised concerns over the privacy and independence of an individual. In the European Union (EU), protection of data is considered a fundamental right, and the General Data Protection Regulation (GDPR) acts as a new structure to protect that right. This regulation creates a very positive atmosphere for the consumers and enables the Europeans to have complete control over their personal information. The General Data Protection Regulation (GDPR) is seen as a role model by other countries as they implement their own laws to protect data. The GDPR provides a comprehensive data protection law for processing of personal data.

WHAT IS GDPR?
[1]The General Data Protection Regulation is the core of Europe's digital privacy legislation and the most inclusive data protection and privacy regulation till date. It creates detailed rules for how personal data is composed, moved, administered, and kept. The foremost purpose of this regulation is to abridge the regulatory atmosphere so both the citizens and the businesses in the European Union can fully benefit from the digital economy. Overriding the **Data Protection Directive (DPD)**, it was drafted and passed by the European Union (EU) and was put into

[1] GDPR decoded https://www.gdprdecoded.com/gdpr-primer

effect on May 25, 2018 and enforces severe fines on those who will encroach upon its security and privacy standards, with penalties up to tens of millions of euros.

Data plays a very important role in our day to day life. From social media, companies, to banks and governments, every service that we use contains the analysis and collection of our personal data. From our name to our address, credit card number and much more are composed and perhaps most prominently, kept by organizations. Under the GDPR regulation, organizations have to guarantee that the personal data is assembled legally and under strict circumstances, and those who gather and manage it are obliged to protect it from exploitation, and misuse, as well as to respect the rights of data owners. There are two different types of data-handlers that the regulation applies to:

-Processors

-Controllers

A **controller** is a person or a public authority who alone or in association with others gathers personal data and also explains what will happen with the personal data, while a **processor** is an individual or public authority which processes personal data on behalf of the controller.

The controllers and processors must take suitable practical and administrative actions to execute the data protection principles. While designing the information system they should keep privacy in mind. Processing of data should be done under one of the six lawful bases quantified by the regulation, they are: (Consent, public task, contract, vital interests, legitimate interest, or legal requirement). And when the processing is grounded consent, the data subject has the right to withdraw it at any time.

WHAT DATA DOES THE GDPR APPLY TO?

The GDPR basically applies to [2]personal data.

Personal data means any information relating to the data subject or consumer, which can be used to identify them directly or indirectly. This information can consist of anything from a name, an e-mail address, a photo, biometric data or the IP address of a person's computer. Whether or not, the IP address is considered personal data under GDPR has been a subject of debate. The lawmakers then made it clear that IP address will come under personal data as the identity of a person can be traced from his IP address.

Data that has obvious personal identifiers like first name and last name can also come under the GDPR depending on the fact that how hard it is to conclude the identity of an individual from that data.

SENSITIVE PERSONAL DATA

The GDPR makes sure that the processing of personal data which reveals a person's racial or ethnic origin, his/her opinion on politics, religion and philosophy or trade union membership as well as the processing of genetic and biometric data for the purpose of identifying a natural person and the data relating to a person's health, his/her sex life or sexual orientation shall be prohibited.

The above mentioned, statement will not apply, if the individual has specifically given his/her permission for the processing of their data, or under a few other specified circumstances.

[2] What does the GDPR basically applies to https://www.dataselect.com/who-does-the-gdpr-apply-to/

DATA INVOLVING CRIMINAL OFFENCES

Under the GDPR regulation the processing of data which is related to criminal convictions and offences or security measures shall be carried out only under the supervision and control of the official authority or when the processing activity is authorized by the Union or a Member State Law provided that they lay out appropriate safeguards for the rights and freedoms of the data subjects. Comprehensive record of criminal convictions shall be kept under the supervision and control of the official authority.

In order to process personal information about criminal offences or convictions, there should be a lawful basis under Article 6 and an official authority for the processing under Article 10.

DATA CONCERNING CHILDREN

The GDPR contains provisions intended to improve the protection of children's personal information and to ensure that children are addressed in a clear language that they can understand. When it comes to children's data protection, transparency and accountability plays a very essential role, especially when they are accessing online services.

WHO WILL BE IMPACTED?

This regulation applies to organizations functioning within the EU as well as any organization outside the EU which offers its goods and services to the customers or businesses in the EU. Which means t[3]hat almost every major business in the world needs a GDPR compliance strategy. This new regulation is proposed to offer individuals with better control over their data now that businesses are accumulating additional personal data.[i]

LAWFUL BASES FOR COLLECTION OF DATA

These [4]lawful bases were adapted from the 1998 Data Protection Act's 'conditions for processing', and under the GDPR we can only process data, if we can produce both written as well as procedural evidence of at least one of the six lawful bases, which include:

1. **Consent**:

Consent is the sturdiest of all the lawful bases because it talks about the main motive of GDPR, that is, to give an individual full control over their personal data. In essence, a clear permission must be obtained from the individual for the processing of their data for an explicit purpose.

2. **Contract**:

The processing of data is necessary to enter into a contract with the data subject. And if the processing activity is not comparable to the terms of the contract, then the data processing activity requires to be covered by a different legal basis. This will be the basis used when payment details have to be processed.

3**. Legal Obligation**:

The processing activity has a legal requirement, such as an employment, information security or consumer transaction law. For example: A court order may require an individual to process his/her personal data in order to comply with its ruling. When a person quotes their legal obligation, it's a

[4] The six lawful bases for collection of data https://www.cbronline.com/list/6-lawful-bases-for-processing-data-under-gdpr

good idea to also state what statues or agencies he/she can report to.

4. **Public task:**

This means to collect information in the public interest, such as performing a task given by a public authority. Usually, it doesn't apply to private companies, but also doesn't require statutory power for the processing of data. An individual cannot claim this basis if they can get away without the processing of data.

5. Legitimate Interests:

The processing activity is important for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to guard the persons personal information which supersedes those legitimate interests. This base will not apply to a public authority processing data to perform their official tasks.

6. Vital Interests:

This basis refers to the processing that is absolutely necessary but also a case where consent doesn't apply. This interpretation of the basis states that a person can reply on this basis if they need it to protect someone's life but he/she can't otherwise get consent for the processing activity.

GDPR COMPLIANCE?

It [5]refers to the act of ensuring that, business practices and operations will align with the regulations as instructed by the GDPR.

GDPR TERMS AND CONDITIONS

There are six important principles under GDPR. These principles concerning the processing of personal data are present under Article 5 of the GDPR. According to this Article personal data shall be based on:

1. Principle of Lawfulness, Fairness and Transparency

Under this [6]principle special emphasis is given on personal data being managed in such a way that provides a clear explanation for those individuals whose information is being composed and managed. In this principle;

a. An organization must establish a lawful basis for collecting data to process it.

b. Data should be administered **lawfully, fairly and in a transparent manner** with respect to the data subjects.

c. Collection of data should be done only for **specified and legitimate** purposes and not for any other purposes.

2. Principle of Purpose limitation:

Under this principle, it is important for an organization to have a policy on the collection of personal data and that the personal data is being used for a specified purpose with the prior consent of the data subject and in not being misused or exploited.

3. Principle of Data minimization:

Many organizations collect and store large amounts of data for different purposes, be it marketing tenacities, research, monitoring actions. Under this principle, regardless of the size of an organization or the type of data stored in that organization, it is advised that the organizations must assess the significance of the information stored and that any data held has to be limited to only which is required by the organization for explicit purposes.

4. Principle of trueness, accuracy:

Under this principle, organizations must have a far-reaching policy and procedure for regular reviews to enable GDPR principles

[5] GDPR Compliance https://www.compliancejunction.com/gdpr-compliance/

[6] Principles of the GDPR https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en

compliance with this principle. All organizations will be required to maintain an accurate database of all the customers and employees.

5. Principle of integrity and confidentiality:

This principle completely deals with security. It is the accountability of the organization to guarantee that all the necessary measures are taken to protect the personal information that their data subjects hold. Such as unlawful use, unintentional damage as well as external threats such as malware, phishing or theft. Weak security systems could be subjugated, causing distress to the individuals. Under this principle, the GDPR conditions that the organizations should have the suitable levels of safety to address the risks presented by their processing.

6. Principle of storage limitation:

According to this principle, an organization cannot collect unnecessary information which is not pertinent to the objective of the collection. So, before collecting any kind of data, organizations must figure out exactly what they need. There should also be periodic reviews, so that unnecessary data can be removed after a certain period of time.

INDIVIDUAL'S RIGHTS UNDER GDPR

Under the GDPR, the following [7]rights are provided to the individuals:

1. The right to be informed

- Individuals should be well informed about the collection and processing of their data. This is a transparency requirement under the GDPR.
- Individuals have the right to know about the purpose collection of their data and with whom their data will be shared.
- Privacy information should be provided to the individuals during the collection of their data.
- If personal data is obtained from any other source, then the individuals must be provided with privacy information within a period of one month.
- If an individual already has the necessary information then there is no need to provide privacy information to them.
- Information provided to the individual's should be accurate, transparent and easily accessible.

2. The right of access

- Individuals have the right to access their personal information. This is known as subject access. The request for a subject access can be made verbally or with a written request. An organization has about one month to respond to that request. And in most cases, no fee is charged.

3. The right to rectification

- Individuals can get their data complete, if its incomplete. The request for the completion of their data can be made verbally or in writing.
- An organization has one month to respond to this request.
- In certain situations, an organization can chose to reject this request.

4. The right to erasure

- The data subjects can have their personal information erased. This is also known as **'the right to be forgotten'**.
- Request can be made verbally or in writing. Responding period is one month.

[7] Individuals rights under GDPR https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation

- This is not an absolute right and can only be used in certain circumstances.

5. The right to restrict processing

- Individuals have the right to request the restriction of their personal data. This is not an absolute right and can only be applied in certain cases.
- Request can be made verbally or in writing. Responding period is one month.
- When processing is restricted, an organization can store the data but they cannot use it.

6. The right to data portability

Individuals can reuse their personal data for their own purpose across various services.

- They can easily transfer their personal data from one IT atmosphere to another.
- This allows individuals to take advantage of applications and services that can use this information to acquire them a better deal.

7. The right to object

- Individuals have the right to object to the processing of their personal data in certain circumstances.
- They have an absolute right to stop their personal data being used for direct marketing.
- Organizations must tell individuals about their right to object.
- Request can be made verbally or in writing. Responding period is one month.

COUNTRIES WITH GDPR-LIKE DATA PROTECTION LAWS

1. California Consumer Privacy Act (CCPA) – USA

- [8]This regulation was enacted in 2018 and took effect on January 1, 2020
- Provides additional rights and protections regarding how businesses may use their personal information
- It imposes many restrictions on businesses that are similar to those required by the General Data Protection Regulation (GDPR)

Rights for California customers:

- Right to know about the main aim of collection of data
- Right to delete personal data
- Right to forbid the sale of personal data
- Children under the age of 16 have to give clear consent to have their data eligible for sale
- Guarantee that individuals who perform their rights under the CCPA will not be penalized with higher prices than those who do not

2. LEI GERAL DE PROTECAO DE DADOS (LGPD) – BRAZIL

- Also known as the Brazilian General Protection Law;
- Passed by the National Congress of brazil on August 14, 2018 and comes into effect on August 15, 2020.
- Closely modelled after the GDPR
- Their definition of personal data is similar. The LGPD has stated in various places that personal data can mean any data which could identify a person or subject them to a specific treatment and in this one place it is more extensive than GDPR.
- Their fundamental rights are also similar to each other. The GDPR has 8 fundamental rights and the LGPD has 9 fundamental rights, despite the different count, they are essentially the same rights.

3. THAILAND PERSONAL DATA PROTECTION ACT (PDRA)

- Approved by the National Legislative Assembly of Thailand in February 2019
- Published in government Gazette on 27 May, 2019 and came into effect on 27 May, 2020

[8] Countries with GDPR like laws https://insights.comforte.com/9-countries-with-gdpr-like-data-privacy-laws

- The PDPA and GDPR are similar to each other in;
- Definition of personal data
- Establishment of legal basis for gathering and usage of personal data
- Harsh penalties and fines
- Extraterritorial applicability

4. PERSONAL INFORMATION PROTECTION ACT – SOUTH KOREA

- This regulation has been in effect since September of 2011 and has included various GDPR like provisions. These provisions are;
- Gaining consent
- Scope of valid data
- Appointment of a Chief Privacy Officer
- Limitation of data retaining period

DATA PROTECTION LAWS IN INDIA

In [9]India, as of now, there is no legislation or a specific law that deals with the subject of data protection or on the violation of privacy of an individual. Some sections of the Information Technology Act which was passed in 2000 by the parliament and amended in 2008, deals with computer related offences or crimes and violation of privacy but these provisions are not sufficient to deal with the present scenario. The Information Technology Act, 2000, addresses issues relating to monetary compensation (civil) and penalty (criminal) in the situations of misuse of personal data and the violation of contractual terms on personal data.

India presently has a comprehensive personal data protection bill that is under discussion in a joint parliamentary committee, which has many consent-related provisions that are quite similar to those enshrined in the European Union's General Data Protection Regulation (GDPR).

This bill states that in order to gather personal information those entities that are classified as data fiduciaries must acquire permission from the individuals whose data is being talked about. Data fiduciaries are any entity who determine the purpose and the means of processing personal data. This definition includes everything from ride-sharing apps to social media to data brokers that purchase and resell client data.

This [10]bill further levies extra requirements, such as an obligation to obtain the consent of the parent or the guardian for the assemblage of information belonging to children. The bill also carves out a number of exceptions for when the data fiduciaries may not have to acquire consent in order to gather personal data. For instance, in order to comply with court orders there are exceptions for state or other entities, enforcement of law and medical emergencies.

The provisions of the bill also give rights to data principles, those about whom data are being collected. The data principles can request information from the data fiduciaries about the collection of their personal information. The data principles also have the right to correct or erase their data stored by the fiduciary – a "right to be forgotten," which is also mentioned in the GDPR. They will also have the right to view their data in a clear and transferable manner, with the data presented in a structured format.

SUPREME COURT JUDGEMENT ON RIGHT TO PRIVACY

[9] Overview of data protection laws in India http://www.ehcca.com/presentations/privacysymposium1/steinhoff_2b_h1.pdf

[10] Data protection bill in India https://www.prsindia.org/billtrack/personal-data-protection-bill-2019

Justice K.S. Puttaswamy vs Union of India and others, 2017

[11]Justice Puttaswamy, a retired High Court Judge, filed a writ petition in 2012 against the Union of India before a nine-judge bench of the Supreme Court challenging the constitutionality of Aadhar on the grounds that it is violating the right to privacy. The issues raised by him were:

1. Whether or not there is any fundamental right of privacy under the Constitution of India?
2. Whether or not the verdict given by the court that there are no such fundamental rights in M.O. Sharma & Others. vs Satish Chandra, DM, Delhi & others and also, in kharak Singh vs The State of U.P, is the correct expression of the constitutional position?

The nine-judge bench of the Supreme court of India passed a landmark judgement on 24th August 2017, upholding the fundamental right to privacy under Article 21 of the Constitution of India.

Article 21 of the Constitution states that:

"No person shall be deprived of his or personal liberty except according to procedure established by law".

It was stated in the judgement that the term 'privacy' is to be an integral constituent of Part

III of the Indian Constitution, which lays down the fundamental rights of the citizens. The apex court also stated that the state should carefully balance individual privacy and the legitimate aim, at any cost as fundamental rights cannot be taken away by law, and every law and act must abide by the Constitution. The court also added that the right to privacy is not an absolute right and any invasion of privacy by state or any non-state actors must satisfy the triple test:

1. Proportionality
2. Legality
3. Legitimate Aim

This judgement proved that the Supreme Court of India once again appeared as the sole protector of the Constitution in creating a legal context for the protection of privacy in India.

CONCLUSION:

Taking into consideration, all the above qualities, the General Data Protection Regulation (GDPR) turns out to be a major success in enhancing the privacy and data security of the European Union citizens and turns out to be an ideal role model for other countries, who themselves are trying to build a stronger data protection laws for the betterment of their citizens.

It is very important to protect our personal data and information from third parties as personal information can be used for exploiting a person's reputation and can be used to influence our decisions and shape our behavior. For instance- Recent data breaches by top service providers like Facebook, Twitter among others have raised serious questions on whether personal information of an individual is safe or not? In the [12]Cambridge Analytical scandal wherein data of millions of Facebook users was leaked and was allegedly misused by Cambridge Analytica (a data mining firm which was linked to Donald Trump's Presidential campaign) created a sense of dissatisfaction across the world including India, which is

[11] Justice K.S. Puttasswamy (Retired). Vs Union of India And Others., 2017. Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1 https://lawlex.org/lex-bulletin/case-summary-k-s-puttaswamy-retd-v-s-union-of-india-2017/18929

[12] Cambridge Analytica and Facebook: The Scandal and the Fallout So Far https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

one of the countries with highest number of Facebook users. Due to situations like this it is very important for a country to have stronger and stricter data protection laws as the more someone knows about us, the more power they can have over us.

*****