

# INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

---

Volume 2 | Issue 1

2020

---

© 2020 *International Journal of Legal Science and Innovation*

Follow this and additional works at: <https://www.ijlsi.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

---

This Article is brought to you for “free” and “open access” by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication at **International Journal of Legal Science and Innovation**, kindly email your Manuscript at [editor.ijlsi@gmail.com](mailto:editor.ijlsi@gmail.com).

---

# The General Data Protection Regulation (GDPR) A Tool For Technological World

---

KRITIKA GOSWAMI AHUJA

## ABSTRACT

*“If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people’s accounts. If they know there’s a key hidden somewhere, they won’t stop until they find it.*

*” – Tim Cook, Apple’s CEO.*

*However keeping the above in mind one can say that the technology although have significant positive impacts on the human life but its negative impact on people’s privacy cannot be overlooked hence it’s the responsibility of the people as well as the government to keep their data security on priority basis. On this basis the European Union has tried to guarantee the security of this directly through enactment. Therefore, in 1995 the European Union took its first step in lieu of the protection security standards by legal enactments. Since then the rule regarding the data protection has evolved and in 2018 the general data protection regulation also known as GDPR came in force. GDPR came into force to meet the needs of emerging data protection issues. However, many other countries have also made an attempt to make legislative framework for the protection of data breaches made by companies. India too has very recently made few attempts and has found a way to establish a data security structure displayed along the lines of the GDPR. The term GDPR stands for general data protection regulation. GDPR are the set of rules and regulations which govern the people and the economic areas of EU. In this article an attempt is made to understand concept of GDPR alongwith its impact and the challenges brought in its implementation. Further other data protection models are also brought into the consideration to get a better understanding of GDPR Model.*

## I. INTRODUCTION

Technology has significantly changed human life however with the growing development in the area its negative effect can't be overlooked. Consequently this drove approach to compelling lawful authorization. Hence, the EU also recognized the requirement for modern protection and therefore, in 1995 it passed the European data protection directives which led down the basic data protection and security measures upon which each member state based

its own executing laws. The basis of these Directives were derived from European convention on human rights, 1950. These directives were drafted in the mid-90s and faced significant changes in the manners by which individuals utilized data, both in business and individual contexts. Hence to make Europe fit for new, by data protection laws. On May 25, 2018 GDPR came into force to meet the needs of emerging data protection issues. The term GDPR stands for general data protection regulation. GDPR are the set of rules and regulations which govern the people and the economic areas of EU. In other word, GDPR are the legal framework which sets the guidelines for the protection of a natural person by imposing obligations onto the business entities responsible for collecting and processing the private information of the citizens or European economic area of EU. The term “personal data” means any information relating to an identified or identifiable natural person, 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.<sup>1</sup>

## **II. GDPR APPLIES TO?**

GDPR applies to any organisation processing personal data within or outside European Union. It also includes processing activities related offering of goods and services, monitoring of behaviours of data subjects within union.

## **III. BENEFITS OF GDPR**

- GDPR provides transparency and gives individual prominent authority over how their personal information should be dealt with. To elaborate we can say that it gives the consumers a sense of security which boosts their confidence on their data custodian organisation.
- It improves data security. As it mandates each organisation to have data security offers and in case of any breach occurrence the organisation will have to give information within 72 hours.
- It removes irrelevant data which no longer is required hence it's effective in data cost maintenance.

---

<sup>1</sup>Article 4 (1) General Data Protection Regulation 2018.

#### IV. DISADVANTAGE OF GDPR

- Implementation of GDPR led to various problems also one of it is increase in cost compliance as it created an unforeseen salary add-on data protection officer.
- It also led dis-interest of many of the organisation due to over regulations.

#### V. GDPR AND THE LAWS GOVERNING DIFFERENT COUNTRIES

##### 1. GDPR AND INDIAN LAWS

In the present scenario the companies across the world are trying to figure out the impact of GDPR on their corporate world. Indian companies are too in this league of finding out the impact it will cause on Indian economic structure if the GDPR style laws are implemented in India. . In July 2017, the government of India appointed a Committee of Experts on a Data Protection Framework for India, or Data Protection Committee (DPC), under the chairmanship of Justice B.N. Srikrishna, to study issues related to data protection in India.<sup>2</sup> Though the committee submitted its reports in 2018 but it faced certain challenges. Thereafter the committee proposed an updated draft personal data protection bill (also known as PDPB). This bill contains some major changes in comparison to its first draft. The PDPB model drives its basis from the European model of GDPR. In PDPB Model the extension of application of scope is more extensive than that of the GDPR, as an entity may fall inside extension just by handling individual information in India. Further the definition of personal data is also broader in comparison to GDP Model. In addition to this the PDPB model grants the government broader authority to compel the disclosure of information which does not constitute to personal data.

Currently the only law which is governing the social platform in India is protected under the Information Technology Act 2000. In 2009, S.43A was embedded by an amendment to keep up with stringent data protection laws prevailing in Europe as “this was adversely affecting outsourcing”.<sup>3</sup> Further, another legal recognition towards consumer data protection is the step taken by supreme court in *K.S Puttaswamy And Others Vs Uoi And Ors*<sup>4</sup> the right to individual identity or in other words right to privacy was also considered as an important part of fundamental right to life under Art 21.

---

<sup>2</sup> Committee of Experts under the Chairmanship of Justice B N Srikrishna, “Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna,” Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018), [https://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report-comp.pdf](https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf).

<sup>3</sup> Pg.189, Chapter 8, Data Security and Privacy, Cyber Law, Indian & International Perspectives on key topics including data Security, E-commerce, Cloud Computing and Cyber Crimes, 2012 Edition, Aparna Viswanathan

<sup>4</sup> [HTTPS://INDIANKANOON.ORG/DOC/127517806/](https://indiankanoon.org/doc/127517806/) SEPTEMBER 26, 2018.

Keeping in mind the recent steps taken by the Indian government on 29 June 2020 to protect the data privacy on social platform by banning certain apps it can be said that it is the need of hour that the Indian government should enacted regulation on data protection and it's better to have one even if flawed than to none.

## **2. US DATA PROTECTION LAW VS GDPR**

The United States has no such one in all formulated law, it work on a different approach and hence the two cannot be compared.

## **3. CALIFORNIA CONSUMERS PRIVACY ACT (CCPA) VS GDPR.**

CCPA ensures the data protection of California consumers from business entities that meets the specific threshold limits. Based on the GDPR model the CCPA also is different in certain aspects. However, the ccpa differs from GDPR in its scope as it stops the organisation from sale practises. In other words it stops the companies to sell the personal data of individuals by providing link on their home page.<sup>5</sup> Further the ccpa only to for profit business (small scale businesses are exempted) whereas the GDPR applies to any sort of business, organisations etc. Furthermore, the penalties are more in GDPR in comparison with CCPA.

## **VI. CHALLENGES IN IMPLEMENTATION OF GDPR**

The challenges of GDPR implementations widely dependence on various factors such as:

- Understanding the scope of applications of. As many non- EU companies fail to understand its scope that how GDPR applies to them or whether they come under the ambit of GDPR or not.
- Many companies lack the appropriate framework for establishing GDPR and fail to understand as to whom they should provide with data information.
- No data removal period is mentioned hence the organisation fail to deal with the issue of irrelevant data removal which led to data cost maintenance.

## **VII. PENALTIES**

Article 83-84 deals with the infringement of GDPR by imposing general administrative fine. However, section 4 lists the infringement which comes under the purview of administrative fine which is 10 million or 2% of companies global annual turnover. Further, section 5 of article 83 provides with higher fine of 20 million or 4% of global annual turnover.

## **VIII. CONCLUSION**

The GDPR is an aggressive and spearheading endeavour to make complete, uniform standards of security and data protection. The issues related to it are intricate and as an effective tool it will keep maturing according to the changing requirement. In conclusion to the above it can be said that GDPR is a major advance to the brilliant fate of the cutting edge individual information showcase and it should be considered as an opportunity for the high tech business organisation to gain advantage in future completely controlled market, expand on client dependability and trust.

\*\*\*\*\*