Page 3095 - 3103 **DOI:** *https://doij.org/10.10000/IJLMH.11843*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Data Protection Regulations in European Union

PAVAN KUMAR.R[1]

ABSTRACT

Data protection laws can be traced back to 1970, The importance of data security and the need to regulate privacy will grow as the global economy evolves increasingly toward a linked information landscape. Understanding diverse ways to developing more compatible legal frameworks at the national, regional, and global levels, as well as various paths for doing so, is critical international trade facilitation and internet commerce facilitation. New technological developments have resulted in adding urgency to this need. Cloud computing has quickly risen to prominence, disturbing traditional models in various areas of law, business, and society. , GDPR replaced the EU's previous data law adopted in 1995 even before Google was even registered as a domain name. This Article aims in analysing the EU GDPR provisions. Where GDPR needs businesses to be more accountable to the data subjects or the individuals whose data they collect and imposes much tougher punishments for those who fail to comply with. GDPR will also be an important contribution to the development of global data standards. This article further emphasises on the data processing, the rights of the data subjects, the safe harbor rule, and the data protection impact assessment.

Keywords: *GDPR, Data Protection Directive, Data Processing, Data Controllor, Safe Harbor Rule.*

I. INTRODUCTION

The Data Privacy field is growing rapidly, and its impact is already seen. Protection of individual rights was recognised under International instrument of Human rights that is Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life.[2] In other words human rights development in EU was because of influential nature of UDHR. In the human research context, modus operandi for legitimate action is considered as Consent and it serves as a powerful ethical as well as legal norm, it is most important requirement in research such as clinical trials, but consent to participation in research is not the same as that of consent serving as the legal basis for transformation under Data Protection Legislation.

[1] Author is an Associate at Dr. Gubbi House of Justice, India.

[2] Article 12 of United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948.

 [ISSN 2581-5369]

With Treaty of Lisbon in 2009 coming into effect, the Charter of Fundamental Rights of the EU became legally enforceable, and with this the right to the protection of personal data was uplifted to the status of a separate fundamental right. Data protection laws have grown rapidly, more than 108 nations have either fully or partially accepted Data protection laws or given effect to the laws in their domestic jurisdictions. On May 25, 2018, which is considered as important day for Privacy laws, as the General Data Protection Regulation (GDPR)[3] took full fledge legal effect across the European Union (EU) and, subsequently, the European Economic Area (EEA)[4] which includes 31 countries, its impact on European Union and around the globe is enormous.

EU laws are composed of treaties such as Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), which is considered as 'primary EU laws' along with the secondary EU laws, this secondary EU laws are nothing but the regulations and the decisions of EU which is adopted by EU institutions.

The principle EU legal instrument on data protection is of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data, where harmonisation of data at national level is one of the main objective behind the Data Protection Directive.[5] This directive is designed in such a way that it gives sanctity to the Privacy provisions which was specified in the Conventions. The Data Protection Directive extend to both EU members and Non- EU member states that are part of the European Economic Area (EEA).[6]

(A) Key definitions

There exist many key definitions in GDPR few of them are considered here:

1. Personal data: It is an information where individuals can be identified directly or indirectly. For e.g. Names of the individual, location, biometric data, religious beliefs, etc.

2. Data processing: Any action of processing done on the collected data whether automated

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR]

[4] Decision of the EEA Joint Committee No 154/2018 of July 6, 2018 amending Annex XI (Electronic communication, audio-visual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]. Membership of the EEA has grown to 31 states as of 2018: the 28 EU member states (which still includes the United Kingdom at the time of writing), as well as three of the four member states of the European Free Trade Association (EFTA): Iceland, Liechtenstein, and Norway. The other EFTA member, Switzerland, has not joined the EEA, but has a series of bilateral agreements with the EU that allows it also to participate in the internal market. Switzerland is currently revising its Federal Act on Data Protection to accord with the GDPR and maintain its "adequacy" status under Art. 45 of the GDPR.

[5] Data Protection Directive, Recitals 1, 4, 7 and 8

[6] Agreement on the European Economic Area, OJ 1994 L 1, which entered into force on 1 January 1994.

 [ISSN 2581-5369]

or manual. E.g. recording, organizing, structuring, storing, using.

3. Data subject — The person whose information is processed. E.g. client or website visitors.

4. Data controller — Data Controller is a person who decides why and how personal data will be processed.

5. Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has emphasised on special rules for these individuals and organizations.

II. CONCEPT OF PERSONAL DATA

'Personal Data' is defined as an information relating to identified and identifiable natural person,[7] which means the information of the person is manifestly clear, such person may be called as "data subject". The jurisprudential nature of Article 8 of ECHR says that it is quite difficult the differentiate the matters of personal and professional life.[8] Natural person is always the beneficiary of the Data Protection Laws. In Amann v. Switzerland,[9] *"The ECtHR found that the interference in the applicant's case had not been in accordance with the law since domestic law did not contain specific and detailed provisions on the gathering, recording and storing of information. It thus concluded that there had been a violation of Article 8 of the ECHR."* Rights enshrined under ECHR is not only applicable to natural person, but also to others, as the matter of professional life is subject to data protection. Under Convention 108, the Data protection laws is applicable only with respect to natural person, but it may be extended to Legal entities if the contacting parties agree to extend the Data protection laws.

However, EU Data protection laws never emphasise on protecting legal person, regarding the data processing which are concerned to them, they can do so with the consent of National Regulators.[10] In Volker and Markus Schecke and Hartmut Eifert v. Land Hessen,[11] CJEU held that "*legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons*."

Personal Data covers private life information as well as information with respect to professional life. Sensitive Data is a special category of the Personal Data, where it poses risk on the individual is disclosed. The definition of sensitive data, under the purview of Convention 108

[7] Data Protection Directive, Art. 2 (a); Convention 108, Art. 2 (a)
[8] See, for example: ECtHR, Rotaru v. Romania [GC], No. 28341/95, 4 May 2000, para. 43; ECtHR, Niemietz v. Germany, 13710/88, 16 December 1992, para. 29.
[9] ECtHR, Amann v. Switzerland [GC], No. 27798/95, 16 February 2000, para. 65.
[10] Data Protection Directive, Recital 24.
[11] CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen, 9 November 2010.

 [ISSN 2581-5369]

(Article 6) and the Data Protection Directive (Article 8) name the following categories:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions, religious or other beliefs; and
- Personal data concerning health or sexual life.

In addition to the above the details of convicts of the criminal case, the memberships of trade unions, medical details of the patience with vulnerable diseases are sensitive data under the Data protection Laws.

III. GENERAL DATA PROTECTION REGULATION

Outside the European Union, very few jurisdictions have data privacy frameworks that are aligned with OECD guidelines or GDPR. Under GDPR the most important accept is getting the consent, which is considered as essential for an agreement of the Data subject. GDPR is now considered as new gold standard in the field of Data protection laws.

Some other significant enhancements to GDPR that will empower the consumer include:[12]

1. Audit trail: Companies must keep track of when and how people grant their consent.

2. Right to be forgotten: Under certain circumstances, GDPR gives individuals the power to get their personal data erased i.e. If consent is withdrawn, there is no legitimate interest, or it was unlawfully processed, it is no longer essential for the purpose for which it was gathered. In this case, the controller, and others with whom they shared your information must guarantee that it is completely removed. Automated decision-making: In few cases, individuals have the right not to be subject to decisions based on automated processing without any human intervention.

3. Data portability: GDPR allows individuals to request that their data be sent to another controller so that the data subject can make more use of it. Further applications might include analysing bank transaction data for spending trends and insights, as well as transferring contacts from one network to another. This is a new development that has arisen through GDPR which was quite missing from the previous data protection directive which was followed in EU.

4. Transparency of data collection and transmission: Companies clearly specify that how they collect the information from the data subject. What is the actual purpose the data is used and the different ways the data will be processed?

[12] The state of data protection rules around the world: A briefing FOR CONSUMER ORGANISATIONS

5. Accessing your data: Individuals will no longer be charged to access their data and shall have the right to access any information a company holds on them within thirty days of asking. They can also ask for that data, it can be rectified if its incorrect or incomplete.

6. Data breach notification: Company's Breach detection and response protocols must be able to detect and respond to breaches as soon as they occur. Within 72 hours of becoming aware of a data breach, companies must notify both their data protection authorities and the persons impacted by the breach, including complete facts of the breach and a proposal for limiting its consequences.

7. Data Protection Officer: Companies of a certain size that frequently and systematically monitor or process substantial amounts of data must appoint a data protection officer who will function as a point of contact for workers and customers with data protection questions. GDPR defines pseudonymisation as "the processing of personal data in such a manner that it can no longer be linked to a specific data subject without the use of supplementary information." The word pseudonymisation is not found in Data protection Directive, whereas it can be found 15 times in GDPR. Pseudonymisation is an encryption which is to translate identifiable parts of personal data to unique artificial identifiers, so-called pseudonyms.[13]

IV. PERSONAL DATA PROCESSING PRINCIPLES

Personal Data processing principles are quite like that of GDPR personal Data Protection Principles. On April 27, 2016, the European Union adopted the GDPR, more than four years after the European Commission proposed it. Which came into effect on 24th May 2016.[14] And shall be applicable from 25th May 2018 on the day, Data Protection Directive is nullified. GDPR explicitly requires data to be processed in a transparent manner and it defines both "processing" and "personal data", whereas Data Protection Directive implicitly requires data to be processed. Further, GDPR will either rectify or erase the inaccurate data without any sort of delay.[15] Accountability principle enables the controller to demonstrate the compliance with other Data protection laws.[16] The controller determines the means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. GDPR places specific legal obligations on the processors and ensures the contract between processor and the

[13] The General Data Protection Regulation Long awaited EU-wide data protection law is now applicable, by Deloitte.
[14] GDPR, Art. 99(1), at 87 ("This regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union."). The date of its publication in the Official Journal of the European Union was May 4, 2016.
[15] GDPR, Art. 5(1)(d).
[16] GDPR, Art. 5(2)

GDPR is complied. For archiving purposes like historical research or statistical research purposes, public interest, GDPR has established specific regime for personal data processing.[17]

V. LEGITIMATE PROCESSING

GDPR develops "Purpose Limitation Process" by allowing the controller to evaluate whether personal data processing for a purpose other than the one for which the data were originally collected enjoys such a basis, where it is not based on the law or the data subject's consent.in order to do so GDPR has retained the existing, legitimate basis must exist in order for personal data processing to be legally valid.[18]

The GDPR on the other hand defines data subject "consent" but provides the additional requirement that the data subject's wishes be "unambiguous" and manifested "by a statement or by a clear affirmative action."[19] Where the consent must be free from ambiguity, has its an necessary element of processing basis. The controller should establish that data subject has given consent.[20]If a consent request is included in a declaration that includes other topics, the request must be properly expressed and identifiable from other topics, with one risk of noncompliance being that the consent request will be nonbinding.[21]

GDPR ensures, data subjects should be informed about their right to withdraw consent prospectively, and such right should be easily accessible because the consent is initially given by the Data subjects.[22] When accessing whether data subject has freely given consent, a reviewing authority shall consider, If contract performance is "conditional on authorisation to the processing of personal data that is not essential for the performance of that contract," "utmost account" should indeed be taken.[23] With respect of processing a juvenile under the age of sixteen is only lawful if "the holder of parental responsibility over the child" provides or confirms consent. Member states may reduce this age limit to no less than thirteen years old.[24] The controller should verify that such holders have given consent or not.

VI. RIGHTS OF DATA SUBJECT

GDPR Article. 8(1), needs transparency in the provision of information to data subjects about their rights and the means of exercising them, it is regardless of whether data is collected by

[17] GDPR, Art. 5(1)(e).
[18] GDPR, Art. 6.
[19] GDPR, Art. 4(11)
[20] GDPR, Art. 7(1)
[21] GDPR, Art. 7(2)
[22] GDPR, Art. 7(3)
[23] GDPR, Art. 7(4)
[24] GDPR, Art. 8(1), The age sixteen threshold specified in this provision does not affect the general law relating to the legal capacity of a child to enter a contract. Id. art. 8(3).

 [ISSN 2581-5369]

Data subject[25] or indirectly from Third Party[26]. When it comes to rights of the Data subject, GDPR follows few provisions of rights that was enshrined under Data Protection Directive, such as right to object to processing,[27] right to access,[28] right to rectification "without undue delay",[29] right to erasure ('right to be forgotten').[30] The right of forgotten is dependent on data subject based on the criteria set out in relevant clauses and may become irrelevant when right of freedom of expression and information,[31] based on public interest. Right to restrict processing may apply, for a specific time period as set out in Article 18 of the GDPR. EU law may confine certain data subject rights to safeguard, among other things, national security, Défense, and furtherance of justice.

VII. IMPACT ASSESSMENT

As per GDPR, the controller must conduct Data Protection Impact Assessment ("DPIA"), DPIA is required when processing sensitive data categories, data relating to criminal convictions of the data subject and in order to do so requires four fundamental elements:[32]

- Processing should be a systematic description.
- Assessment of the respective risks referred to above.
- measures to address the risk (including safeguards, security measures, and mechanisms to ensure data protection and regulatory compliance); and
- an assessment of the "necessity and proportionality of the processing operations in relation to the purposes."

In case where DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller must consult with the concerned authorities.[33] The controller or the processor must be designated based on expert knowledge he posses in the field of Data Protection law, they ae bound by the principle of confidentiality with respect to the data subjects.

VIII. NOTIFICATIONS OF DATA BREACHES

Controller should notify any kind of Data Breaches within 72 Hours, once he is aware of such

[25] GDPR, Art. 13.
[26] GDPR, Art. 14.
[27] GDPR, Art. 21, Compare Directive 95/46, Art. 14,
[28] GDPR, Art. 15, Compare Directive 95/46, Art. 12,
[29] GDPR, Art. 16, Compare Directive 95/46, Art. 12(b)
[30] GDPR, Art. 17; see also Voss & Castets-Renard, at 297–98, 334–36 (terming the "right to be forgotten" as including a "right to digital oblivion")
[31] GDPR, Art. 17(3)(a),
[32] GDPR, Art. 35(7).
[33] GDPR, Art. 36(1)

 [ISSN 2581-5369]

breaches without any undue delay, unless otherwise provided by the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, unless exceptions provided.[34]

IX. PENALITIES

As per GDPR, substantial fines shall be charged for those who are at fault of Data protection violation. In circumstances up €20 million or 4 percent of the entire world wide turnover of the previous financial year whichever is higher.[35] The concerned companies with there supervisory committee may try to reduce the fine or the penalties that are being imposed for their data protection violation, while doing so they should give due regards to, any action taken by the controller or the processor to mitigate the damages suffered by data subjects, when the controller or the processors responsibility considering the technical and organisational measures implemented by them, adherence to approve certification measures.

X. SAFE HARBOR PRINCIPLE

Data protection Directive emphasised that the data can be transferred to third country, which intend to undergo processing, provided that the third country ensures an adequate level of protection.[36] In the year 2000, the European Commission and the U.S department of commerce negotiated EU-US safe harbor in order to transfer the personal data to U.S companies which had complied with the rules of EU data protection laws. In *Schrems v. Data Protection Commissioner*,[37] ECJ held that access to personal data by U.S. authorities in connection with mass surveillance and later invalidated the Safe Harbor, which left thousands of companies without a legal basis for their cross-border personal data transfers.[38] Court of Justice of European Union, further was of the opinion that the national supervisory authority must examine the data protection carefully as it is concerned with the personal rights of the data subjects, and found that European Commission's Safe Harbor decision denied these powers to the DPAs.[39] Which resulted in invalidating the EU- US Safe Harbor where the US companies were processing the personal data's.

[34] GDPR, Art. 34(3)
[35] GDPR, Art. 83(5)
[36] Directive 95/46, Art. 25(1)
[37] Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015), http://eurlex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:62014CJ0362 (accessed on 29-05-2021)
[38] Mark Scott, Data Transfer Pact Between U.S. and Europe Is Ruled Invalid, N.Y. TIMES, http://nyti.ms/1jLWfwc. (accessed on 29-05-2021)
[39] Supra note 36.

 [ISSN 2581-5369]

XI. RIGHT OF DELISTING

In the Google Spain Case,[40] court permitted a data subject the right to compel delisting of newspaper pages containing data detrimental to him once internet users sought for his name using a search engine. The French data protection authority ("CNIL") sought to have the delisting extended to all relevant domains, including ".com," while Google wanted to limit the right's geographic reach to European web domains. The CNIL has issued a directive to that impact, which Google disputed, causing the CNIL to open a formal investigation. CNIL restricted committee imposed a cost of €100,000 on Google. According to the CNIL, "only delisting on all of the search engine's extensions, independently of the extension used or the geographical origin of the person doing the search, can adequately uphold" the right to privacy.[41]

XII. CONCLUSION

The main important aspect of privacy is the processing data is processed securely. EU has adopted GDPR, which is the data protection reform in the present times, GDPR provisions highlight company's compliance requirements and call for more responsibility and documentation. Companies can now self-certify under the Privacy Shield for cross-border personal data transfers. They should keep an eye on changes affecting the right to be delisted, since this impacts Internet access to information. In general, the GDPR standards differ from analogous standards in the United States, many of which are state-by-state required and include various definitions and remedies for data breaches.[42] Supervisory authority under the GDPR model are designed to enforce and provide guidance on privacy laws across the EU. Thus, GDPR draws attention to protection of personal data. It introduces specific changes that where not seen in the earlier Data protection laws. GDPR also provides the option to exchange data with third countries without suitable safeguards. This is possible if there is a legally binding instrument between the government authorities. Which means GDPR assures to privacy protection to the internet users.

*****

[40] Case C-131/12, Google Spain SL v. Agencia Espan˜ ola de Proteccio´n de Datos (AEPD), 2014 E.C.R. 317,
[41] Right to Be Delisted: The CNIL Restricted Committee Imposes a €100,000 Fine on Google, CNIL (Mar. 24, 2016), https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposeseu100000-fine-google [hereinafter Right to Be Delisted, https://www.cnil.fr/sites/default/files/atoms/files/d2016054_penalty_google.pdf.
[42] Reynolds A. GDPR matchup: US state data breach laws. International Association of Privacy Professionals. May 2018. https://iapp.org/news/a/gdpr-match-up-u-s-statedata-breach-laws.