International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

GDPR: A Privacy Regime

Pranaya Dayalu, M. Punnagai

Student, B.B.A., L.L.B. (Hons.), Shanmugha Arts, Science,
Technology & Research Academy, Thanjavur, Tamil Nadu, India

How to cite this paper: Pranaya Dayalu | M. Punnagai "GDPR: A Privacy Regime" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.713-716, URL: https://www.ijtsrd.com/papers/ijtsrd23460.pdf

IJTSRD23460

ABSTRACT

Privacy is not a choice and it should not be the price played for our access to internet. We live in an era where everything is digitalized and anybody and everybody, from a child to a 70 year old accesses the same on a regular basis. Great advances in the technological field constitute a greater danger to the privacy of every individual. The constant question that arises is whether the data principal consents to the information provided and disseminated? Mercerization of personal information has opened pits of security breaches and data privacy problems. When one consents to provide his data, does he consent to the dissemination of the same? The very idea that consumers must make a trade-off between privacy and security has been wiped away by the very enactment of the General Data Protection Regulation. This paper stands as proof that, GDPR is the answer to all the data privacy questions and problems faced by the society. The author briefs through the history of enactment EU GDPR and its necessity. The paper brings out both the endless advantages of GDPR as well as the few disadvantages present. The extensive research on GDPR has prompted the author to attract attention to the key changes seen after the implementation of GDPR and the robust data privacy regime built by its awakening. The main cerebration of the authors by referring to the above submissions is that GDPR is a need of the hour and is for the betterment of the society as a whole.

Key Words: *data protection, privacy, surveillance*

INTRODUCTION

GDPR is a new set of rules designed to give European Union citizens added control over their personal data and businesses in the EU fully benefit from the digital economy. GDPR applies to all organizations operating both within and outside the EU which offer goods or services to customers or businesses in the EU. General Data Protection Regulation is a regulation in EU law on privacy laws and data protection for every individual in European Union and the European Economic Area. GDPR replaced the data protection directive to bring in a much better and standardized legislation for data privacy protection.

Privacy has been a major concern in the past, it continues in the present and will be in the future too. Hence a more significant law has been introduced in the European Union's history called The General Data Protection Regulation (GDPR) which is the resultant of rigorous discussions about the privacy arrangements and numerous amendments of previous directives. The successor of 1995 Data Protection Directive, GDPR gives liberty for varied interpretations and implementations to meet its requirement. Despite these opportunities given, in meeting its specific requirements, GDPR is stringent, the trans-border scope, the privacy in its design, and also in addition to numerous other requirements. GDPR also sets outlooks and benchmarks for developing privacy laws and regulations across the world.

GDPR's provisions are made in a way that any personal data of citizens exported outside the EU is protected and regulated. It mainly gives two rights the right of erasure, or the right to be forgotten. If data is not wanted out there, then you have the right to request for its removal or erasure. Second, the right of portability, the notices to users must be very clear and precise as to its terms, when it comes to "opt-in/opt-out" clauses.

TIMELINE

- In 2016, EU adopted the General Data Protection Regulation (GDPR), replacing the 1995 Data Protection Directive which was adopted at early stages of internet.
- In 1980, the Organisation for Economic Co-operation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" in order to create an extensive data protection system throughout Europe.
- In 1981 the Convention made for the Protection of Individuals regarding Automatic Processing of Personal Data was negotiated within the Council of Europe but its obligations regarding data protection was duly did.

The European Commission proposed the Data Protection Directive realizing the diverging data protection legislation amongst EU member states that impeded the free flow of data within the EU.

According to this directive personal data should not be processed at all, unless met by certain conditions. These

conditions to be satisfied fall into three categories: transparency, legitimate purpose, and proportionality. Personal data can be transferred to third countries only if that country provides an adequate level of protection.

- On 25 January 2012, the European Commission (EC) announced to unify data protection law across a unified European Union via proposed legislation called the "General Data Protection Regulation." The EC has set conformity date on 25 May 2018, giving a chance to business organisations to prepare for compliance, reviewing data protection language in their contracts, considering transition to international standards, update privacy policies, and review marketing plans around the world.

GDPR OVER DIRECTIVE 95/46/EC

On comparison made between the directive and GDPR, the directive has certain territorial restrictions as it is mainly within the union itself, however it provides certain protection outside EU but with many restrictions ensuring adequate level of protection required from the third nation. Also another reason or replacing the directive is that it has restrictions in material scope also. Does not apply to processing of personal data for activities which lie outside scope of Union law and by competent authorities in relation to criminal offences and penalties and threats to public security and also Under Regulation (EC) No 45/2001. This needs to be adapted for consistency with GDPR.

The GDPR adds social security and social protection when it comes to processing of personal data which is not mentioned in directive. When the consent comes into question in the predecessor Data Protection Directive, it is more than enough to have ambiguous consent. DPD also includes implementation of pre contractual measures taken upon data principal's request. Processing does not require identification and it does not comply with the Directive. The DPD lacks the position of Data protection officer and Supervisory Authority. Under GDPR the data principal has been conferred the right specifically. This is not so in DPD as it merely obliges the supervisory authority to hear claims concerning rights and freedoms.

According to *Art.94 GDPR*: The Directive 95/46/EC is repealed with effect from 25 May 2018

1. References to the repealed Directive shall be construed as references to this Regulation.
2. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Member States are entitled to provide specific rules or to the GDP and the entry into force of the GDPR requires updating EU regulations, such as the revision of the E-Privacy directive to regulate the confidentiality of communications and the use of cookies.

The EU's 1995 data protection rules for strengthening online privacy rights and boosting Europe's digital economy was later proposed by the European Commission with an extensive reform . This includes the organisations established outside EU that offers goods and services and have control over the individuals in EU. The European Data Protection Supervisor adopts protection reform package to bring accountability.

ENACTMENT OF GDPR

The Article 29 Working Party adopts an Opinion for data protection through explicit consent on March 23, 2012. This makes consent necessary to legally access the individual data by the organisations. Individuals may withdraw their consent at any time.

On October 5, 2012 the article 29 of work party made the Organisations to notify data breaches if that is likely to pose a risk for individuals to their data protection authority within 72 hours and they will have to inform the affected individuals also.

By March 12, 2012 The European Parliament got strong support for GDPR by voting in plenary with 621 votes in favour, 10 against and 22 abstentions. The processing organisations were established in several member states with supervisory authority.

The European Data Protection Board replaced the articles formulated by the working party, who are the co-legislators and made several recommendations in the final text of GDPR. The European Parliament, the Council and the Commission reached with an agreement on the GDPR on December 15, 2015.The GDPR ensures preservation of the individual data when transferred outside of union and it can be done only with their consent.

GDPR reinforces a wide range of existing rights and establishes new ones for the protection of individual's privacy that includes the right of data portability and right to not to be profiled. The European Commission proposes two new regulations on privacy and electronic communications (E-Privacy) and on the data protection rules applicable to EU institutions (currently Regulation 45/2001) that align the existing rules to the GDPR.

A new Proposal for Regulation on the protection of personal data in EU institutions was made on May 22, 2018 repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

The General Data Protection Regulation came into existence on May 25, 2018 and was implemented on the very same day. Every organisation in EU were mandated to comply with GDPR and had to appoint a Data Protection Officer to ensure they comply with the GDPR.

During the first few weeks of implementation of GDPR it is said that global data regulators faced several challenges like Governance and accountability, Enhanced data subject rights, Transparency and information requirements, Data portability and subject access requests, Records of processing activities, Application to non-EU organisations, Data protection impact assessments, Data breach notification, Cross-border discovery, Enforcement against non-EU entities.

DATA PRIVACY PROTECTION

Personal data as defined by Black's Law Dictionary is any part of information that is recorded about an individual person. Includes the name, email, address, ethnicity, race,

identifying number, employment history, etc. GDPR turned to be a paradigm shift in data protection and privacy.

Privacy has been a major area of concern in the past, continues to be so in the present and may remain so in the future. As computerized disruption keeps on testing protection standards over the world, cloud, online networking and versatile innovation headway is generally modifying the individual and expert existences of individuals over the globe. The concerns around data privacy is on both ends, that is, the consumers as well as the enterprises. The consumers on one hand are concerned about misuse of their privacy and sensitive personal data as well as critical personal data, the enterprises are concerned having a dampening impact on their , brand value, consumer trust as well as revenues.

With the GDPR coming into force from 25 May 2018, organizations need to evaluate their processes as to see their standing in their data privacy journey as the onus of accountability rather shifts from regulators to organizations. As per the 6 main legal grounds for lawful processing, organizations need to understand and document what data is acquired, maintained and processed, and the legal basis for it.[2] This standardised increase in accountability ensures better protection of sensitive personal data of the data principal.

With GDPR, EU occupants have more control over their own information as associations will be considered in charge of the information they process and they will likewise need to get unequivocal assent from the inhabitants to process it. One of the key focus area for organisations across the globe is GDPR compliance. As per the reports[3], there has been a 50% increase in the number of complaints since the legislation came into effect as compared to the corresponding period last year.

With the implementation of EU GDPR organisations have come up with better privacy protection budgets and thereby establishing a secure data privacy regime. We live in a world of constant surveillance. Generally, this has been expensive and difficult to comprehend. However in this highly technological era, surveillance has progressed by a wide margin with its tentacles encompassing each part of the current virtual world, wherein everything is either procured, saved, analysed or looked over the web. The GDPR compliance is based on both technological and legal aspect. Through the mandatory obligations placed by the GDPR on data processors through Articles 27 to 31, the privacy of every data principal is safeguarded hence moving much closer to a better data privacy regime in the era of surveillance.

GDPR KEY CHANGES

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. The EU GDPR being a successor of the former EU Directive consists of key changes such as:

- **Increased Extraterritorial Applicability**:

The most drastic change seen through the implication of GDPR in the landscape of data privacy is the extended territorial jurisdiction of GDPR, as it now applies to all organisations processing personal data of data principals residing in the Union regardless of their geographical location. Formerly, territorial jurisdiction in the Directive was more ambiguous and referred to the processing of data in the context of an establishment, whereas

GDPR is clear in its terms and applies to the processing of data by controllers and processors in EU, irrespective of their place of establishment.

- **Penalties**

Organisations which have breached the GDPR guidelines can be fined up to 4% of annual global turnover or €20 Million, whichever is greater as per Art. 29 of EU GDPR.

- **Consent**

The consent of data principals as to the procurement and processing of data has been strengthened and organisations can no longer trap the users with the lengthy terms and conditions full of legalese. Consent must now be distinguishable and clear and must be provided in an easily accessible form, using plain and clear language.

- **Data Subject Rights**

GDPR has brought in a highly secure standard through the implementation of breach notifications, right to access and right to be forgotten. Through breach notification any breach with the compliance of GDPR must be notified within 72 hours of such a breach as this breach of data privacy is violative of fundamental right of privacy of individuals.

Right to access enables the data principal to know everything from the procurement to the processing of his data by the controller. Through right to access the data principal can now request certain personal data to be refrained from being processed and the controller must provide the data principal with the copy of the processed data free of charge when requested for the same.

The game changer in GDPR is the Right-To- Be-Forgotten also known as Data Erasure which entitles the data principal to have the data controller erase his personal data, stop from further dissemination of personal data and halt potential third parties from procurement and using of such personal data.[4] Though this right is subject to an exception in favour of public interest in the accessibility of such data.

- **Data Protection Officers:**

GDPR has mandated the internal record keeping and has thereby appointed DPO for those processors and controllers whose core activities consists of systematic processing on a regular basis. Otherwise a DPO is not mandatory.

MERITS AND DEMERITS:

GDPR proved to be the need of the hour which was seen as an opportunity to build consumer trust. GDPR like any other regulation and legislation had its share of merits as well as disadvantages, the former more than the latter.

[2] https://www.i-scoop.eu/gdpr/legal-grounds-lawful-processing-personal-data/

[3]https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-sharp-rise-in-complaints-after-gdpr

[4] Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (2014).

The advantages of GDPR are:

- The CIO of UK gave that businesses can obtain a "competitive advantage" if they "get data protection right". This is so because the processing and procurement are now systemized and follow a particular legalese.
- GDPR is essentially about trust and builds more consumer relationships. This is an added advantage as consumers previously feared for their data security whereas that breach is now solved with the implementation of GDPR.
- Organizations are now accountable for any GDPR non-compliance resulting in a breach of any sort majorly data privacy and protection of sensitive personal data.
- With the enforcement of GDPR right to privacy which never existed has now become a fundamental right of every individual and cannot be abridged in the name of data processing and dissemination.
- With data accountability it acts as onus to prove the risks taken by the companies in the processing of data. This accountability further builds loyal consumer chains. Accountability encapsulates everything GDPR is about.[5]
- Furthermore, GDPR has acted as a catalyst and driven improved cyber resilience. In an annual cyber security breach survey organizations in UK said that the cyber risk has reduced to 32% from 43% the previous year. Proliferations of cyber hacks have come down and GDPR has acted as the base not only for data privacy but also for cyber security.
- The territorial applicability has extended drastically with the implementation of GDPR so as to involve procurement and processing of data irrespective of the location. Data localization has changed in great leaps and bounds with the added spread of territorial jurisdiction. This promotes cross border transfers and aides in the dissemination of data.
- This is a regulating measure which enables everyone across the EU Union to process data without the diversified legislations which pose as a restriction. It harmonizes dissemination and growth of data privacy and security and easy transfers.

The very few yet very much present demerits of GDPR are:

- This overregulation of EU through GDPR leads to red tape in the form of endless consent requirement. This over burdens the users with easy access that too in an era of user friendliness.
- A major drawback of GDPR is the cost effectiveness. Upon implementation of GDPR every organization is now mandated to frame new guidelines in compliance of GDPR and implement the same which require a great amount of budget. Organizations are now required to allocate separate privacy budgets to achieve the objective of GDPR. It is not enough if the companies alter their internal affairs, rather they have to now appoint DPOs for the millions of data they procure and process.
- The penalty for non-compliance has been a major concern among every other organisation, though the very same penalty is what encouraged the companies to consider their data protection responsibilities.

CONCLUSION

GDPR, an extensive leap in the realm of data protection and privacy as seen in this paper is a much needed one and is here to stay irrespective of its few drawbacks. GDPR rewrites the entire cyber security standards and holds companies accountable for failure to protect EU citizens' data in the eyes of law. As already proven by the 2018 statistics there has been a subsequent decline in data privacy and security risks after the implementation of GDPR and this number will keep declining once all the compliances are met with by organizations. GDPR is an excellent venture for organizations to gain trust of their consumers and build a loyal base thereby gain a competitive advantage. In order to conclude the authors would like to assert that GDPR is a major breakthrough from the former head-in-the-sand approach towards data privacy and one which guarantees privacy as their fundamental right as well as provides with cyber security.

[5] https://www.out-law.com/en/articles/2019/april/ico-businesses-fail-gdpr-accountability-/