JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

COMPLIANCE THAT PROMOTES PROTECTION OF PEOPLE'S DATA

Anushree Agrawal, Dr. Sarvesh Mohania
PhD Scholar, Associate Professor
Jagran Lakeview University

Abstract **–** In this era of digitalization, where personal data is being constantly collected and processed, protection to individual's privacy is of utmost importance. General Data Protection Regulation which came into existence in 2018 has brought a wave of data protection throughout the world. It aims to provide control to the individuals over their personal information. This regulation demands for certain standards to be complied with. However, such standards seem general in nature but if an organisation needs to comply with such standards or to initiate such program, it involves multiple steps, various measures which needs to be taken into consideration and the multi-level processes that needs to be implemented has been discussed in this paper. This paper also highlights the role of key players in General Data Protection Regulation compliance. GDPR compliance serves as a cornerstone for building a secure and ethical digital landscape that respects individual's privacy rights while promoting innovation and economic growth.

Index Terms **- Compliance, data subjects, personal information, Privacy, privacy program.**

I. INTRODUCTION

As stated by Kevin Plank, Data is a new oil. It is transforming the world into digital world. In this digital world, everything is digital data driven which has brought the revolution. In this era where almost, everyone has the smart phones and are on social apps irrespective of the fact of their age, gender, financial status or culture, data has been shared by each one of us by ignoring the fact that how, where and for what purposes this data will be used and what could be its repercussions. This ignorance has costed many corporates and individuals hefty charges in last decade.[1] These scams have led the urge of having a robust law to protect one's data. This has given rise to General Data Protection Regulation (GDPR) in May 2018 in European Union.

The evolution of GDPR has brought the organisations throughout the world under the extended scrutiny with regards to their privacy practices. Legal and regulatory requirements, ethical obligations, consumer pressure and highly competitive environment have made them to implement the requirements to protect the data rights of the subjects. This calls for the GDPR compliance. Following the trend, many other countries including India has come up with similar laws for their country but GDPR has become the benchmark.

As we know, GDPR compliance is about adhering with the practices and processes that helps in protecting the data subject's rights. In this article, the researcher has intended to highlight the process of GDPR compliance by the organisations. For the purpose of writing this Article, researchers have primarily used the secondary source of the data.

II. WHY GDPR COMPLIANCE

GDPR is a regulation on data protection and privacy in the European Union (EU) and European Economic Area (EEA). It has been formulated with the purpose of providing protection to a natural person regarding the usage and movement of their personal data (General Data Protection Regulation, n.d.). GDPR has extra-territorial applicability. Meaning thereby the GDPR will be applicable on the non- EU establishments if they are involved in doing business with EU people or their data as per Article 27 of GDPR.

GDPR has changed the way the personal data has to be processed and organised by introducing self-regulation of the personal data processing, imposition of hefty penalties, obligation to notify the breach, introduction of data protection officer (DPO), extension of territorial scope, establishment of the process of taking consent (Chaturvedi & Sinha, n.d.; Gupta, n.d.; Poritskiy et al., 2019).

This regulation has come up to provide data protection to its subjects pertaining to their data privacy (Ghosh & Shankar, 2016). Data privacy is about access of the data whereas the data protection is about providing tools and mechanism to access that data. As privacy got recognition and people became more vigilant and conscious about their privacy rights, need for data protection laws

[1] Ani Petrosyan, Statista (Apr 19, 2023), Largest online data breaches worldwide 2023 | Statista, last accessed on July 06th, 2023 at 17:28 PM.

arise. GDPR has been created with the intention of building trust in EU market, smooth working environment for trading, customer friendly and giving data subjects the right to manage their data and transparency and accountability (Godiyal & Singh, n.d.).

III. WHAT IS GDPR COMPLIANCE

Compliance is a state of being in accordance with established guidelines or laws. There are basically two types of compliances: Corporate compliance is the one where an organisation put rules, regulations and practices into place according to external regulations and internal policies and Regulatory compliance is the one where an organisation put rules, regulations and practices into place according to external regulations.

This regulation is based is based on two fundamental principles which has been derived from ISO/IEC standards (Bańka et al., 2021). These principles are:

3.1 Risk based approach

This principle has been originated from ISO 31000: Risk management, ISO/IEC 27005: Information security, cybersecurity and privacy protection (guidance on managing information security risks), ISO/IEC 29134: Security techniques which evaluates risk in order to choose the protective measures. This remains the basis of the standards related to information safety management. Accordingly, the data controller will evaluate the risk related to the processing of personal data, identification of threats related to the processing and infringement of the rights and freedom whose data has been taken. This is done with the intention of reducing the risks by prescribing actions and required technical measures.

3.2 Principle of accountability

This principle originates from ISO/IEC 27001: Information security management systems, ISO/IEC 27002: Information Security Controls, ISO/IEC 29151: Information Technology. This has been considered as equivalent of protection category defined by the standards of compliance. This is with regards to provide compliance with the information protection principles accepted within the organisation. Proper application of this principle ensures that the data controller has implemented the requisite procedures and documentation to be in line with GDPR. This helps an organisation to prove that the requirements to be in compliance with GDPR has been met.

GDPR provides for following rights for individuals (Burri, 2021; Gupta, n.d.):

1) The right to be informed.
2) The right to rectification.
3) The right of access.
4) The right to be forgotten (erasure).
5) The right to restrict the processing of your data.
6) The right to data portability.
7) The right to object.
8) Rights regarding automated profiling and decision making.

GDPR is able to play its role and perform its duties only because of the presence of its key players. Below diagram represents the key players of GDPR.

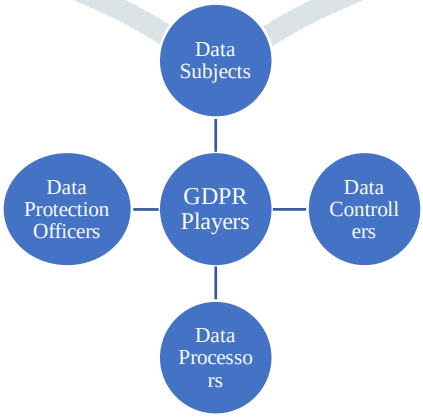

Figure 1: Key players of GDPR

Data Subjects: This term is used to refer to individuals who are natural persons and can be identified.

Data Controller: These are the ones who are responsible for processing of data and also for its protection. Controller is the one who determines different factors which are required for data processing like the purpose, tenure, etc and who and how the data will be processed, what privacy measures needs to be adopted. The significant term here is "control", meaning thereby even if the organisation is not having the possession but is in control of the data then the onus of safeguarding the same lies on them. Data Controller can also appoint the data processor. This has been detailed under Article 24 of GDPR.

Data Processor: It is a service provider who can be a natural or legal person, public authority or any other bodies, who will process the personal data on behalf of the controller. Data controller and data processors are jointly responsible for the protection

of the personal data and failure in compliance will result in penalties to both. Processors are also required to comply with the requisite technical controls and measures as specified in Article 28.

Data Protection Officer (DPO): DPO is a guarantor of data protection compliance in an organisation. Though it is not mandatory for all organisations to have it. Following are required to have one:

- Public companies
- Those that processes data on a large scale or collect sensitive data or data related to criminal convictions or offences.

Article 39 of the GDPR states its functions which are as follows:

1) Supervision of
   - Implementation and application of the policies
   - Implementation of impact assessment.
2) Staff training
3) Record keeping
4) Organisation and coordination of audits
5) He will act as a point of contact for the supervisor authorities
6) Management of the interested party's information and their requests as to the exercise of their rights.

IV. DATA

GDPR provides protection of data. We are talking about data; hence it is important to define here what kind of data been provided protection under this regulation. The term information and data has been used interchangeably but there is a significant difference between the two. An unrefined facts and figures which contains no meaning is called as data whereas the processed data which contains the meaning is called as Information (Yadav & Yadav, 2021). But there are various types of Data (Godiyal & Singh, n.d.; Yadav & Yadav, 2021). Like Public data is any data which is publicly available and does not have any restrictions on its usage, storage, modification. For example: text on government sites. Personal data is the data which helps in identification of an individual. For example: email address, location.

GDPR provides protection to personal information which can identify the person. So, if the characteristics of identification has been eliminated from that information, such information does not fall under the purview of GDPR. Here, two concepts come: one is deidentification and another is anonymization. Deidentification is the process of removal of identifying characteristics from data and anonymization is the process of altering information to a point that makes it impossible to tie it back to a specific individual person.

V. COMPLIANCE PROGRAM

There is no straight jacket formula or procedure which needs to be followed by the organisation to be in compliant with GDPR. GDPR provides for certain operational mechanisms to be adhered. Following are those requirements:

5.1 **Privacy Policy**: this amongst one of the primary requirements to be complied is to have documentation, communication and assignment of responsibilities to take care of the process. An organisation has to create a written privacy policy/ies which has to be in consistence with applicable laws and regulations and contractual obligations to customers, vendors and partners. It should also contain the choice and consent practices, collection of information practices, access practices, third party disclosure and handling practices, security practices, monitoring and enforcement practices followed in the organisation. Assignment of responsibilities to person or a team pertaining to execution and compliance of the policy. Also, proper procedure for review, changes and approval has to be made. In order to keep the team updated and to create awareness, training programs should be arranged. There should be annual privacy risk assessment and also when there are changes in technology infrastructure. Privacy incident management process should be created and maintained.

5.2 **Notice**: under this requirement, it is required to inform the data subjects about the privacy practices which includes notice practices followed by the organisation. Informing the data subjects about the purpose of collecting the information and intention of using such information. It will also notify to data subjects with respect to any changes in the privacy policy, practices or purpose of using and collecting the information. Such notification should be in simple and easy language and in a timely manner.

5.3 **Choice and consent**: it is another significant requirement which talks about the rights of data subjects pertaining to their information and choices available to them. Data subjects should also be informed of the consequences of withdrawal of consent or of refusing to share the information. Consent should always be obtained from the data subjects either implicitly or explicitly whenever the personal information has been collected, for what purpose it has been collected, if any new purpose been added, discloses or transferring the personal or sensitive personal information.

5.4 **Collection**: this requirement talks about the procedures through which an organisation gets the possession of personal information. Information should be collected only for the identified purposes, using fair and lawful means. The information, if, collected through the third party, such information has been collected as per the collection of information policy of the organisation and should be reliable. Data subjects should be informed about the methods for collection of data and type of data collected and if any additional information been collected in a timely manner. This requirement also contains an important criterion which is "data minimisation". Accordingly, an organisation should collect minimal required information from the data subjects which is necessary to meet their objectives and should discard the information which is no longer required for the purpose.

5.5 **Use, retention and disposal**: this is the principle which is required throughout the life cycle of the privacy program. Meaning thereby how, when, where and for what purpose the information will be used has been managed under this principle only. As per this, the data subjects should be informed that their data will be used and retained only till the time it is required to attain the objective and should abide by it. Also, as soon as the collected information is not required, same shall be disposed of in a proper and secure manner and the respective data subjects should be timely informed about the same.

5.6 **Access**: this is the requirement under which the data subjects right to have access to their correct information, which is also called as right to redress, has been provided. The procedure for accessing, reviewing, updating and correcting the data has been provided. Access to information should be subject to the authentication of an individual's identity and in an understandable format. Such access should be provided within a reasonable period of time and if required, on a reasonable charge. If any accessibility has been denied to the data subject, sufficient reason should be provided and should be informed of appeal rights, if there is any. Such updated information should be shared with the third party, if there is any.

5.7 **Disclosure to third parties**: this is the requirement which provides guidelines pertaining to the handling of information while sharing or transferring it to the third party for the purpose of doing business. Data subjects should be informed about the third-party disclosures and for what purpose such disclosure been done. Third party who has been assigned with the task of collecting/processing of the information of the data subjects should comply with the privacy policy of the organisation and should work as per the provisions of the agreement. Information with third party can be disclosed without notice or for purposes other than those disclosed in the notice only when it is permitted under the law. Organisation should implement procedures to verify that the privacy controls of the third party are functioning effectively. In case of mishandling of information, remedial action should be taken by the organisation.

5.8 **Security practices**: privacy program which has been developed to protect the personal information of the data subjects has to be safe. Security of personal information can be assured by taking precautions to protect the privacy of their personal information. Protecting the security of personal information is deeply entwined with protecting the privacy of that information. Developing, documenting and implementing an information security program that addresses the majority of privacy related areas of security. ISO compliances are internationally recognised standards to follow the best practices.

5.9 **Monitoring and enforcement**: privacy practices that have been created and implemented needs to be monitored in a timely manner to ensure effective operations. Under this, an organisation should have a mechanism with regards to dispute resolution, how a data subject can approach for queries, complaints or disputes regarding privacy practices. Regular monitoring of the privacy policies and documenting of the cases, if any, been raised with regards to the violation of privacy policies and the corrective action taken against the same, development and implementation of remedial plan for any issues that have been came up at the time of privacy compliance reviews. Also, based on risk assessment, regular monitoring of the privacy program should be done.

VI. CONCLUSION

To protect the privacy of personal information, there is no fixed solution. An organisation which is developing a privacy program for the first time needs to put considerable effort in designing that program, implementing appropriate privacy controls and monitoring the program's effectiveness to ensure that it continues to meet the organisation's legal obligations and privacy objectives. To achieve the objective of privacy program, it is important to include information security, human resources, marketing, legal, procurement and other specialists. It is important to bring these stakeholders together into the process to leverage the expertise of those functions to achieve privacy objectives. Also, every organisation has a unique culture and navigating that culture is important to achieve the objective of privacy program along with bringing up the stakeholders and specialists and create and implementing a full proof program.

REFERENCES

[1] Bańka, M., Soczyński, T., & Wasiak, D. (2021). Practical Methods of Implementation for the Indispensable Mechanism of GDPR Compliance. *Wroclaw Review of Law, Administration & Economics*, *11*(2), 31–47. https://doi.org/10.2478/wrlae-2021-0013

[2] Burri, M. (2021, November 12). Digital Trade: In Search of Appropriate Regulation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3962165.

[3] GDPR and India: A Comparative Analysis — The Centre for Internet and Society. (2017). https://cis-india.org/internet-governance/blog/gdpr-and-india-a-comparative-analysis.

[4] General Data Protection Regulation (GDPR) – Official Legal Text. (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

[5] Ghosh, J., & Shankar, U. (2016). *'Privacy and Data Protection Laws in India: A Right-Based Analysis National Human Right Commission View project Human Trafficking: An Exploration in Greater Kolkata and North Bengal View project*. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspxArticle

[6] Godiyal, S. P., & Singh, K. (n.d.). *A Comparative Study of Data Protection Laws: Current Global Trends, Challenges and Need of Reforms in India*. https://doi.org/10.48001/veethika.2022.08.02.0040.48001/veethika.2021.07.01.006

[7] Gupta, B. K. (n.d.). *General Data Protection Regulations and its impact on Indian Enterprises*. https://www.akgec.ac.in/wp-content/uploads/2020/10/4-Dr_Brijesh_Kumar.pdf.

[8] Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5), 510–524. https://doi.org/10.1108/DPRG-05-2019-0039

[9] Yadav, A., & Yadav, G. (2021). Data Protection in India in reference to Personal Data Protection Bill 2019 and IT Act 2000. *International Advanced Research Journal in Science, Engineering and Technology, 8(8), 251–255.* https://doi.org/10.17148/iarjset.2021.8845

JETIR