Navigating GDPR Compliance: The Intersection of Data Governance, Accountability, and Organizational Culture

Navdeep Singh[1], Shallu Bishnoi[2]

[1]Student, PHD (Law), Lovely Professional University, Jalandhar
[2]Student, LLM, University College Dublin, Ireland

Abstract:
This Abstract highlights the GDPR's important role in shaping data protection practices within the EU and its broader implications for data governance. The GDPR harmonizes data protection laws across EU, establishing comprehensive guidelines for the collection, processing, storage, and transfer of personal data. The GDPR directs significant penalties for non-compliance, thereby reinforcing the importance of adhering to data protection standards. Additionally the GDPR also validates the principles of lawfulness, fairness, transparency, and accountability in the processing of personal data.

INTRODUCTION

The General Data Protection Regulation (hereinafter referred to as GDPR), enforced by the European Union (EU) from May 25, 2018, represents a monumental shift in data privacy regulations, replacing and superseding the EU's 1995 Data Protection Directive (DPD)[1]. This regulation marks the most significant change in data privacy legislation in the past two decades, emphasizing the protection of personal data and privacy rights. It aims to empower EU citizens by granting them more control over their personal data, strengthening their rights, and reforming organizations' approaches to data management. Furthermore, GDPR aims to facilitate cross-border trades and business expansion within the EU while ensuring the free movement of personal data among member states. Ultimately, GDPR seeks to establish a harmonized, unified, and sustainable approach to data protection across the European Union.[2]

The scope of GDPR is extensive, applying to any organization processing the personal data of EU citizens. This regulation significantly broadens the scope from the previous directive, shifting the focus from the location of data processing to the location of the data subject. The GDPR life-cycle commenced in January 2012 with a proposal from the European Commission and was approved on April 27, 2016. However, the EU provided a two-year transitional period for organizations to achieve compliance, allowing them to implement necessary changes until May 25, 2018. GDPR unifies EU rules and laws concerning data protection, establishing a standardized framework for compliance.[3]

GDPR introduces numerous novelties, including the re-definition of personal data, which now encompasses a broader range of information. GDPR defines personal data as "any information relating to an identified or identifiable natural person."[4] The regulation outlines various rights and responsibilities for data subjects (citizens) and organizations (controllers and processors).

Data subjects' rights under GDPR include expanded rights to access, rectify, withdraw consent, erase, and port personal data, as well as the right to object and lodge complaints. Organizations must process citizens' data only with explicit and clear consent and must adhere to strict principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality,

[1] Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 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).
[2] Teixeira, Gonçalo & Mira da Silva, Miguel & Pereira, Ruben. (2019). The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance. 21. 10.1108/DPRG-01-2019-0007.
[3] ibid
[4] Article 4

and accountability. To adhere to this part of the GDPR, it sets out several duties and responsibilities for the parties who are handling this personal data such as controllers and the processors, to make sure the data is managed safely and ethically. Moreover, organizations must conduct Data Protection Impact Assessments[5] (DPIAs) for high-risk data processing activities and designate a qualified Data Protection Officer[6] (DPO) to monitor GDPR compliance and act as a liaison with supervisory authorities. GDPR also mandates reporting data breaches to supervisory authorities within 72 hours and notifying affected data subjects. Compliance with GDPR obligations is crucial for organizations to avoid significant financial penalties and maintain trust with data subjects and regulatory authorities. Next we will discuss the relationship between Data Governance and the obligations of data controllers under GDPR.

Objectives

Some basic objectives of the study are as:

1. To analyze the Data Protection Regulations and role of GDPR as a controlling body in EU.
2. To find out the steps taken by GDPR to Regulate Data Protection in EU.

What is Data Governance?

Data Governance is an essential component of organizations' efforts to ensure compliance with data protection laws and effectively manage their data assets. It involves the application of established principles and practices of governance to oversee and monitor how data is managed within an organization. Drawing on various data management disciplines, Data Governance serves as a coordinating framework to align and integrate data management activities across the organization. Data Governance provides direction and oversight for data management activities by establishing decision rights and responsibilities for data. These rights and responsibilities are designed to meet the needs of the entire enterprise, ensuring consistency and efficiency in data management processes.

Data Governance involves the exercise of authority and control over the management of data assets. It guides how other data management functions are performed within the organization., Data Governance aims to track and enforce regulatory compliance, oversee the delivery of data management projects and services, manage and resolve data-related issues, and promote the value of data assets within the organization.[7]

By implementing robust Data Governance practices, organizations can ensure the effective management of their data assets, mitigate risks associated with data misuse or non-compliance, and leverage data to drive strategic decision-making and business success.

Who is "the controller" as per the GDPR?

Data controller[8] is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The controller plays a central role in the interactions between the various roles, being called into action by the subjects to exercise their rights and being liable in the event of a violation of the rules by the data processors. It is the controller who is generally the organization who handles the data, hence organizational culture plays a crucial role in ensuring compliance under the GDPR. Organizational culture plays a critical role in ensuring GDPR compliance by embedding accountability mechanisms and prioritizing privacy considerations throughout the organization. A culture that values transparency, responsibility, and privacy by design fosters a proactive approach to compliance, enabling organizations to effectively navigate the complexities of data protection regulations and safeguard individuals' rights and freedoms. Thus the GDPR sets out certain duties that a controller must abide by so an organization culture that promotes ethical data governance and protection can be achieved.[9]

[5] Article 35(1) r/w recital 89 and 91

[6] Article 37(1)(b)

[7] Fischer-Hübner, S., Angulo, J., Karegar, F., Pulls, T., "Transparency, privacy and trust – technology for tracking and controlling my data disclosures: does this work?" in Habib, S.M.M., Vassileva, J., Mauw, S., Mühlhäuser, M. (eds.), IFIPTM 2016 (2016).

[8] Article 4

[9] Ibid at 1

Relationship between data governance and the controller under GDPR

The GDPR establishes a comprehensive framework where all key actors are defined and assigned specific roles and obligations. Among these actors, controllers play a pivotal role in ensuring the objectives of GDPR are fulfilled and data is governed ethically within legal bounds. The regulation dedicates articles to outline the obligations of controllers, such as Article 5, 25, 30, 32, and 35. These obligations include ensuring lawful, fair, and transparent processing (Article 5), implementing data protection by design and by default (Article 25), maintaining records of processing activities (Article 30), ensuring the security of processing (Article 32), and conducting data protection impact assessments (Article 35). These obligations serve as foundational elements for organizations to uphold data protection standards, facilitating ethical data governance and compliance with GDPR requirements as given in detail below:-

Under Article 5 of the GDPR, controllers bear significant responsibilities and must adhere to several principles governing the processing of personal data. These principles carry implications for controllers, shaping their data-handling practices and requiring them to demonstrate compliance with the regulation. For better understanding article 5 is bifurcated as follows:-

The accountability principle under GDPR has several implications for controllers:

- Increased Responsibility: Controllers are held more responsible for their personal data processing activities. They are obligated to comply with the general principles of data processing and demonstrate this compliance.
- Risk-Based Approach: The principle promotes a risk-based approach to data protection, allowing for the scalability of data protection obligations, especially in high-risk cases. Controllers are expected to assess and mitigate risks associated with data processing.
- Documentation and Compliance: Controllers are required to maintain documentation demonstrating their compliance with GDPR regulations. This documentation aids supervisory authorities in overseeing data processing activities and facilitates enforcement.
- Enforcement: Accountability enhances enforcement by directing supervision to high-risk processing, setting proportionate penalties, and ensuring that controllers take responsibility for data protection choices.
- Shift in Responsibility: The principle signifies a shift from data subject control to controller responsibility, emphasizing the controller's primary role in protecting personal data.

Overall, the accountability principle places a greater onus on controllers to proactively ensure compliance with GDPR regulations and to demonstrate their commitment to data protection.

In summary, controllers must carefully adhere to the principles outlined in Article 5 of the GDPR to ensure lawful, fair, and transparent processing of personal data. By implementing appropriate measures and demonstrating accountability, controllers can effectively protect data subjects' rights and meet their obligations under GDPR.

Under Article 24 of the GDPR, data controllers are mandated to implement specific measures to ensure compliance with the regulation. These measures must be tailored to the nature, scope, context, and purposes of data processing activities, as well as the risks posed to the rights and freedoms of data subjects.

- Controllers must conduct thorough assessments considering the aforementioned factors to determine appropriate measures. For instance, a healthcare organization processing sensitive patient data must implement stricter measures compared to a retail company processing basic customer information.
- Controllers must deploy technical and organizational measures proportionate to the risks identified. For example, introducing encryption, access controls, and staff training to mitigate risks associated with data processing.
- It's imperative for controllers to regularly review and update implemented measures. This ensures that the measures remain effective in addressing evolving risks and technological advancements.

- Controllers are required to establish and enforce data protection policies within their organizations. These policies outline procedures for data handling, security protocols, and compliance with GDPR requirements.
- Controllers may opt to adhere to approved codes of conduct[10] or certification mechanisms[11] to demonstrate compliance. These frameworks provide additional assurance of adherence to GDPR obligations and best practices.

Records of Processing Activities

Data controllers are required to to maintain detailed records of their data processing activities. These records should document various aspects of data processing, including purposes, categories of data subjects, recipients of data, and data transfers to third countries or international organizations.[12]

Security of Processing

It is the mandates that data controllers implement appropriate technical and organizational measures to ensure the security of personal data. Controllers must protect data against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage.[13]

Data Protection Impact Assessment (DPIA)

Data controllers are required to conduct DPIAs for processing activities that are likely to result in high risks to the rights and freedoms of data subjects. DPIAs help identify and mitigate potential risks associated with data processing, enabling controllers to implement appropriate safeguards.[14]

Data protection by design and by default

It emphasizes the importance of integrating data protection measures into the design and default settings of systems and processes involved in data processing[15]. Key elements are as follows:

- Integration of Data Protection Measures:

Controllers are required to implement appropriate technical and organizational measures at both the time of determining the means for processing and during the processing itself. These measures should be designed to implement data protection principles effectively, such as pseudonymization, and to integrate necessary safeguards into the processing to meet GDPR requirements and protect the rights of data subjects.[16]

- Data Minimization and Default Settings:

Controllers must ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. The aim is to minimize the collection and processing of personal data to the extent necessary for the intended purpose, thereby reducing the risks to data subjects' rights and freedoms.

- Limiting Accessibility of Personal Data:

Controllers must implement measures to ensure that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. This requirement aims to enhance privacy and data protection by restricting access to personal data to only those individuals who have a legitimate need to access it.

- Use of Certification Mechanisms:

Controllers may use an approved certification mechanism under Article 42 as evidence of compliance with the requirements set out in paragraphs 1 and 2 of Article 25. Certification mechanisms provide an additional

[10] Article 40
[11] Article 42
[12] Article 30
[13] Article 32
[14] Article 35
[15] Article 25
[16] The Ethics of Persuasive Technologies in Pervasive Industry Platforms: The Need for a Robust Management and Governance Framework Gustav Borgefalk(&) and Nick de Leon Royal College of Art, Kensington Gore, London SW7 2EU, UK

layer of assurance regarding adherence to data protection principles and can demonstrate a commitment to implementing robust data protection measures.

What happens when the controllers fail to comply?

The case involving Enel Energia, as investigated and fined by Garante, the Italian data protection authority, serves as a significant example of GDPR violations and their implications. The investigation stemmed from findings by the Italian Financial Police, resulting in a substantial fine of €79.1 million, the largest issued by Garante to date. The company faced multiple GDPR violations, including breaches of Articles 5, 24, 25, and 28.

Firstly, Enel Energia failed to conduct an adequate risk assessment of its customer management system and neglected to implement measures to prevent credential sharing by employees, violating Articles 5(1)(f) and 32 of the GDPR. This failure to ensure data security led to serious security deficiencies in the company's information systems. Secondly, the company violated the principles of accountability and privacy by design (Articles 5(2), 24(1), and 25) by allowing illegal activities of other entities attempting to procure contracts, despite knowing they were not part of its sales network. This lack of oversight facilitated illicit business practices and exposed customers to potential harm. Furthermore, Enel Energia's execution of contracts with other entities failed to reflect the actual processing of personal data and neglected to include terms regarding the data controller's obligations, contravening Article 28 of the GDPR.

Garante considered various factors in imposing the substantial fine, including the severity of the violations and the number of individuals affected. Additionally, mitigating factors such as the introduction of an authentication system to prevent credential sharing were taken into account.

In addition to the fine, Garante mandated remedial actions for Enel Energia, including communication of the proceedings' outcome to interested parties, documentation certifying the implementation of security measures, and the introduction of further measures to enhance system monitoring and restrict unauthorized access. Enel Energia was also required to ensure compliance with GDPR terms in contracts with other entities and to report back to Garante within a specified timeframe on the measures undertaken.This case underscores the importance of robust data protection measures and accountability mechanisms to prevent GDPR violations and protect individuals' privacy rights. It highlights the significant financial and reputational consequences that organizations may face for non-compliance with GDPR regulations.[17]

CONCLUSION

In conclusion, the discussion on the relationship between data governance and the obligations of data controllers under the GDPR underscores the critical importance of accountability, ethical practices, and organizational culture in ensuring compliance with data protection regulations. The GDPR, with its comprehensive framework and stringent requirements, places significant responsibilities on data controllers to uphold the principles of lawfulness, fairness, transparency, and accountability in the processing of personal data. Articles such as 5, 25, 30, 32, and 35 of the GDPR outline specific obligations for data controllers, emphasizing the need for proactive measures to safeguard data subjects' rights and freedoms. These obligations extend beyond mere legal compliance to encompass ethical considerations and proactive risk management practices.

Moreover, the case study involving Enel Energia serves as a stark reminder of the consequences of GDPR violations and the importance of robust data governance practices. The company's failure to conduct adequate risk assessments, implement appropriate security measures, and ensure accountability led to significant fines and remedial actions imposed by the Italian data protection authority, Garante. Organizational culture emerges as a pivotal factor influencing GDPR compliance, with leadership commitment, employee engagement, and a strong ethical climate playing key roles in shaping data governance practices. Cultivating a data-driven

[17] Foley, T. (2024). Italy fines energy company over GDPR violations. *Cybersecurity Policy Report,* , 1. Retrieved from https://ucd.idm.oclc.org/login?url=https://www.proquest.com/trade-journals/italy-fines-energy-company-over-gdpr-violations/docview/2967581176/se-2

ethical culture within organizations is essential for fostering accountability, promoting transparency, and mitigating the risks of non-compliance with data protection regulations.

In light of these considerations, it is evident that effective data governance requires a holistic approach that integrates legal compliance, ethical considerations, and organizational culture. By embracing their obligations under the GDPR and fostering a culture of ethical data practices, data controllers can uphold the trust of data subjects, mitigate regulatory risks, and contribute to a data ecosystem characterized by integrity, transparency, and respect for privacy rights.