International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-7, 2020 ISSN No: 2349-5677

IMPLICATIONS OF GDPR ON DATA MANAGEMENT PRACTICES IN COMPANIES

Syeda Hajira Kawsar
syedakawsar@gmail.com

Abstract

The General Data Protection Regulation (GDPR), introduced in May 2018, is a monumental shift in the global data privacy laws. The regulation fundamentally changes how companies manage and process data. It is designed to protect the personal data of the citizens of the European Union but has far-reaching implications outside the European Union, influencing businesses worldwide. This regulation mandates strict standards of transparency, accountability, and user rights that challenge organizations to rethink their strategies regarding the management of data.This paper addresses the GDPR framework, key ideas, and implications for corporate information control practices in governance, compliance, and technological version. It addresses the monetary price, cultural alternate, and complexity of global compliance and different challenges. Opportunities additionally encompass better information first-rate, multiplied believe, and competitiveness might be mentioned. In the light of these recommendations, this paper concludes with the imperative recommendations for companies to ensure proper integration of GDPR principles and practices into their businesses seamlessly to comply and help the world grow sustainably with data economics.

Keywords: GDPR, data privacy, data management, compliance, accountability, data governance, EU regulations, personal data

I. INTRODUCTION

Data has emerged as one of the maximum treasured belongings in the current financial system, riding innovation, personalization, and aggressive strategies throughout industries. However, this accelerated dependence on records additionally brings great responsibility, specially within the protection of individual privacy and ethical use of facts. The European Union's General Data Protection Regulation, applied in May 2018, became a landmark step in the direction of addressing these worries. GDPR establishes a complete framework for shielding non-public data, mandating that businesses handle such information transparently, responsibly, and securely. The regulation applies now not most effective to companies inside the EU but also to any agency dealing with the data of EU residents, irrespective of geographical location [4]. This extraterritorial reach has made GDPR a global benchmark for data privacy laws.The present paper deals with a review of key requirements and far-reaching implications of GDPR for corporate data management practice. It presents the problems businesses face to achieve compliance and the opportunities GDPR can bring to enhancing data governance and consumer

trust. In conclusion, it discusses ways in which companies may align themselves with GDPR operations to remain agile and competitive at the same time.

1.1 Key Requirements and Their Implications of GDPR

- **Transparency and Consent Regarding Data Collection**

GDPR places emphasis on transparency when it comes to data collection, processing, and usage. Organisations should keep people clearly informed about why their data is being collected and what will be done with it [2]. Additionally, firms cannot use overly complex or even vague terms in their privacy policies.

Implications:
This has resulted in companies revisiting their consent systems and privacy notices. Most businesses have invested in interfaces that ensure that users are aware of how their personal data is going to be used. As much as these changes build up user trust, they attract a lot of financial and operational resources, especially for huge data-managing businesses.

- **Right to Access and Data Portability**

GDPR grants individuals the right to access their personal data and request its transfer to another service provider. This provision empowers users and promotes competition by enabling consumers to switch providers easily.

Implications:
Companies need to have systems in place that are able to process access and portability requests in an efficient manner. That requires a lot of technical updates, such as acquiring interoperable formats and being able to ensure security in transfer processes. This is highly costly and time-consuming, especially for companies with scattered systems [1].

- **Right to be Forgotten**

This is also referred to as the right to erasure, where one can request the deletion of personal data when it is no longer needed or consent has been withdrawn.

Implications:
To meet this mandate, an organization needs to establish systems of identifying and deleting data within their systems and databases. For organizations with legacy systems and decentralized data storage, it's a very challenging task to erase data. The corporations ought to additionally stability the proper to be forgotten with different duties by means of law, including maintaining the statistics.

- **Data Breach Notification**

Organizations ought to notify the applicable authorities and the affected people of facts breaches inside seventy two hours in their discovery. This is completed for you to make sure timely motion to save you harm.

Implications
This has expanded the demand for strong cybersecurity controls and incident reaction plans. An organization has to put money into advanced security tools, undertake everyday vulnerability exams, and train employees to come across and respond to breaches The consequences of non-compliance are very severe, including severe fines and reputation damage.

- **Accountability and Documentation**

GDPR requires organisations to show proof of compliance through adequate record-keeping of activities related to data processing, impact assessments, and designating DPOs if required.

Implications
This accountability requirement has driven companies to form compliance teams and have adopted detailed data governance systems. Although these steps improve organisational transparency and efficiency, they add to the bureaucracy and cost.

1.2 Challenges to Companies

- **Financial Burdens**

The implementation of GDPR-compliant systems and processes requires heavy financial investments. This is more pronounced among SMEs, which might lack the resources to implement complex technologies or hire specialized personnel [3].

II. CULTURAL AND OPERATIONAL SHIFTS

GDPR requires an overall shift from a data-centric approach to a user-centric one, favouring individual rights over business interests. This cultural transformation is about re-educating employees, re-defining workflows, and creating an organizational culture that is privacy-conscious.

2.1 Global Compliance Complexities

The extraterritorial nature of GDPR implies that non-EU companies handling the data of EU residents must comply with the regulation. This, therefore, poses challenges in the management of cross-border operations, especially when other jurisdictions have conflicting or less stringent data privacy laws.

- **Technological and Infrastructural Challenges**
  In adopting GDPR-compliant systems, there is often a need to upgrade legacy technologies, to integrate disparate databases, and to apply advanced security measures. All these are resource-intensive tasks requiring technical expertise, and organizations with outdated or fragmented infrastructures find it difficult to comply.

- **Ambiguities in the Law**
  Some parts of the GDPR are vague, such as the definition of legitimate interest. This can cause ambiguity in compliance strategies, and this can increase the chances of unintentional violations.

- **Opportunities Offered by GDPR**
  Indeed, GDPR provides challenges and opportunities for companies to leverage their data management practices on the way to a competitive lead:

- **Building Customer Trust**
  GDPR means that companies can demonstrate allegiance to data privacy, winning the trust and loyalty of clients. This, in turn creates stronger customer relationships and a wonderful brand reputation.

- **Better Data Quality**
  GDPR makes it easy to enhance data management systems within the organizations, thus making them accurate, consistent, and reliable. This helps an organization comply with the regulations and improves decision-making as well as operational efficiency.

2.2 Market Differentiation

Organizations that put forward themselves as privacy-friendly stand out in a competitive market. The proactive adoption of GDPR ensures that organizations attract customers with awareness about privacy and present themselves as leaders in an industry about data protection [5].

- **Better Cybersecurity**
  The focus on data breach prevention and reporting has made organizations invest in robust cybersecurity solutions. These are not only compliance-related investments but also protect the organizations from cyber attacks and the potential financial damage.

- **Long-term Sustainability**
  The adoption of GDPR principles in business practices fosters sustainable growth by bringing organizational activities in line with changing consumer needs and regulatory sentiments.

- **Strategic Recommendations to Companies**
  To correctly deal with the intricacies of GDPR and exploit its possibilities, the following techniques should be taken into consideration:

  - **Invest in Privacy by Design**

    Privacy considerations have to be integrated into the design and development of products and services. This helps make certain compliance from the very beginning and reduces the threat of high-priced retrofits.

  - **Adopt Comprehensive Data Governance Frameworks**

    Implement robust statistics governance frameworks that consist of information high-quality, protection, and responsibility. Conduct regular audits and effect tests to hit upon and deal with compliance gaps.

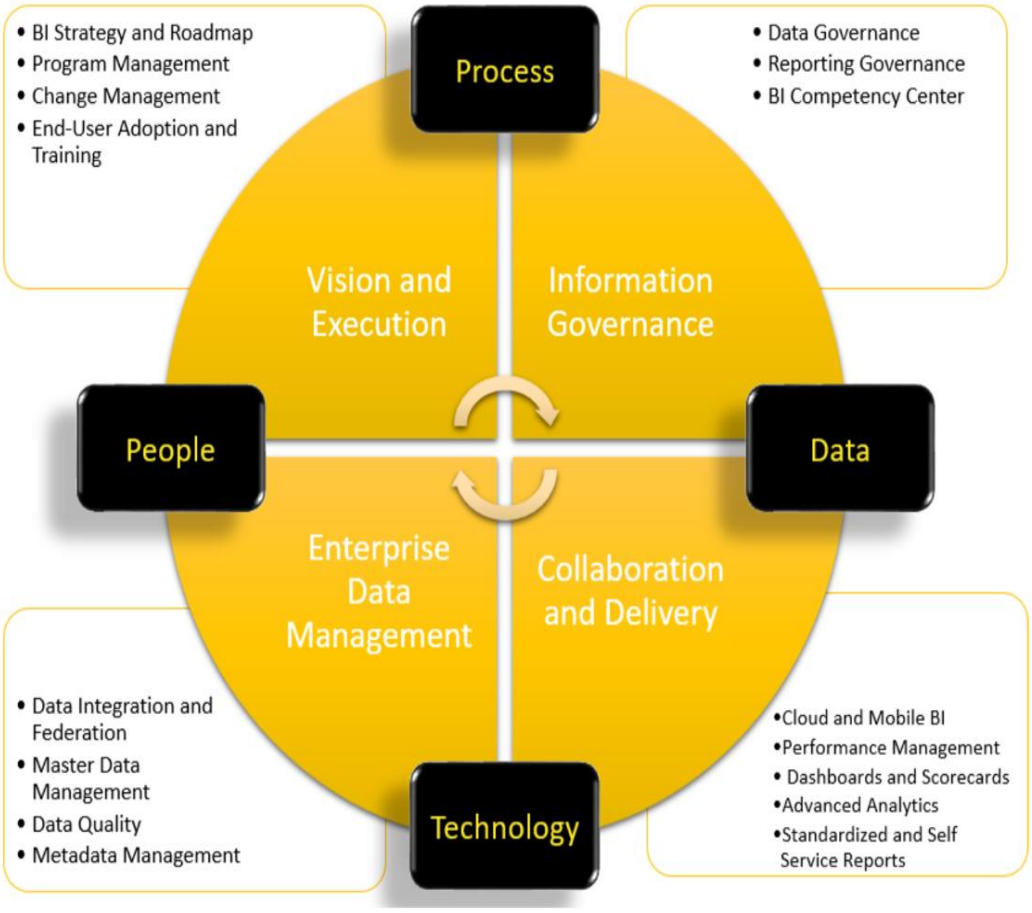

Figure 1: Tips to Ensure Data Governance
(Source:[6])

- **Leverage Technology Solutions**

Apply the contemporary technologies, together with records anonymization equipment, encryption, and synthetic intelligence, to bolster records safety and simplicity compliance strategies.

- **Foster a Privacy-Conscious Culture**

Educate personnel approximately GDPR necessities and the significance of facts privateness. Encourage a culture of accountability and empower personnel to behave as custodians of personal information.

- **Collaborate with Legal and Technical Experts**

Seek to engage criminal and technical specialists to interpret the provisions of GDPR, broaden compliance techniques, and deal with complex challenges.

III. CONCLUSION

The General Data Protection Regulation has dramatically modified the panorama of facts control, setting a new worldwide general for privateness and duty. Compliance isn't always without its challenges, which includes the monetary burden and operational adjustments, but it additionally presents possibilities for corporations to improve their records governance practices, build patron agree with, and advantage an edge over competitors. As statistics privateness maintains to improve, groups should remain proactive in adapting to such alternate and integrating privacy ideas inside their operations. Companies ought to recognize that embracing GDPR now not handiest as a compliance requirement but as a catalyst for innovation and increase will assist them thrive in an an increasing number of data-pushed financial system.

REFERENCES

1. B. Yuan, "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation," International Journal of Environmental Research and Public Health, vol. 16, no. 6, p. 1070, Mar. 2019, doi: https://doi.org/10.3390/ijerph16061070.
2. I. van Ooijen and H. U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective," Journal of Consumer Policy, vol. 42, no. 1, pp. 91–107, Dec. 2018, doi: https://doi.org/10.1007/s10603-018-9399-7.
3. E. S. Dove, "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era," The Journal of Law, Medicine & Ethics, vol. 46, no. 4, pp. 1013–1030, Dec. 2018, doi: https://doi.org/10.1177/1073110518822003.
4. W. G. Voss and K. A. Houser, "Personal Data and the GDPR: Providing a Competitive

Advantage for U.S. Companies," American Business Law Journal, vol. 56, no. 2, pp. 287–344, May 2019, doi: https://doi.org/10.1111/ablj.12139.
5. D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, "Disruptive and avoidable: GDPR challenges to secondary research uses of data," European Journal of Human Genetics, vol. 28, no. 6, pp. 1–9, Mar. 2020, doi: https://doi.org/10.1038/s41431-020-0596-x.
6. Data Governance - Align 1st. (2019, July 31). Align 1st. https://www.align1st.com/think/data-governance/