IJRETM
ISSN-2347 - 7539
International Journal of Research in Engineering Technology and Management

How GDPR compliance created opportunities for enhanced IT governance and digital transformation capabilities.

Dr. Dimitrios S. Stamoulis

Assistant Professor, Business & Technology Department, Webster University, Athens campus, Greece

ABSTRACT: The General Data Protection Regulation (Regulation (EU) 2016/679 is one of the major compliance obligations for all European organizations over the last decade. Its far reaching implications and enterprise-wise span required significant effort from organizations to achieve compliance. Research literature so far has dealt with challenges and enables of GDPR compliance as well as with the significant costs involved into compliance effort. The present study aims at examining GDPR compliance from an opportunity perspective. Based on four interviews with executives from three different sectors of the economy – namely banking, retail and utilities, this paper explores the opportunities opened up by the GDPR compliance project, that led to exploitation of these opportunities towards enhanced IT governance and digital transformation organizational capabilities.

Keywords: *GDPR compliance, compliance driven IT governance and compliance driven digital transformation.*

----------***----------

1. INTRODUCTION

The concept of data protection is of major importance for the respect of privacy, which constitutes a fundamental right for the European Union (EU). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data was a milestone in the history of the legal protection of personal data. The Directive established a comprehensive and detailed framework, for the time, which aimed to ensure the protection of personal data. With the rapid development of the Internet and Information and Communication Technologies in general, on 25 January 2012, the European Commission published a regulation proposal, according to which it proposed a radical revision of Directive 95/46/EC, with the aim of further strengthening data protection. The need for a more comprehensive approach and response became imperative, concluding that "the EU needs a more comprehensive and coherent policy on the fundamental right to the protection of personal data".

The Regulation[1] consists of 99 articles, which define the rights and principles of processing the data of physical persons, the roles and obligations of those responsible and those performing the processing, the rules for transferring data to third countries or international organizations, as well as the Independent Supervisory Authorities, the rules for cooperation and coherence between the parties involved, the responsibilities, the administrative fines and other administrative procedures - functions. To achieve its purpose, the regulation establishes several principles that apply to all kinds of organizations, with significant effort to comply with, proportional to the size of the organizations and the volume of data collected and processed, which personal data can be scattered all across organizational information systems. Comments such as "GDPR compliance has introduced significant costs" (Talens, 2024) and "commentators have recognized that the high costs of putting in place a GDPR-compliant system" (Gal & Aviv, 2020) speak eloquently about the cost side of the GDPR compliance project. Although this was a mandatory project for all organizations due to its compliance nature, organizations are always looking for opportunities in order to balance the incurred costs. These opportunities are hardly researched in the relevant literature so far. This is exactly the aim of this study. Four interviews were taken from executives of three different sectors of the economy that successfully exploited the opportunities revealed on the way towards GDPR compliance. These opportunities led to enhanced IT governance and digital transformation organizational capabilities, which, at the end, turned the cost-benefit balance to the positive side.

In the following section, the main principles of the regulation are presented, along with some examples of their implications. The culmination of the application of these principles is expressed in terms of the data processing subject rights, which constitute the cornerstone of privacy and data protection philosophy of the regulation. Both the principles and the rights, produce ample requirements for organizations to comply with. Then, the main points of the interviews are analyzed, focusing on the different opportunities exploited by the four organizations whose executives were interviewed in a series of dialogues. At the end, summary and conclusions are provided.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

2. PRINCIPLES OF THE REGULATION

Personal data, i.e. any information concerning a person, is divided into two categories, as follows from Article 9. The first category concerns simple personal data, such as name, age, gender, home/work address, email, telephone number, Tax Registration Number etc. The second category concerns special categories of data (sensitive) and refers to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in a trade union, health data and data on sexual life and sexual orientation. Additionally, genetic data, i.e. personal data, relating to the genetic characteristics of a person that were inherited or acquired, as resulting, in particular, from an analysis of a biological sample of that person, are included, as well as biometric data, which result from specific technical processing linked to the physical, biological or behavioral characteristics of a person and which allow or confirm the unequivocal identification of that person, such as facial images or fingerprint data. Given the above, all operations carried out relating to the processing of personal data, as defined in the above section, should be governed by the basic principles set out in the Regulation in Article 5. Those main principles are:

- Lawfulness, objectivity and transparency: Data processing should be carried out within the legal framework and in accordance with the principle of lawfulness.
- The purpose limitation principle ensures that data collection and processing should not be carried out in a manner incompatible with the purposes. Processing for archiving purposes in the public interest or for scientific or historical research purposes or statistical purposes is not considered incompatible with the original purposes.
- The principle of data minimization ensures that data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In other words, organizations are required to limit the collection and processing of data to the minimum necessary, taking into account the context of the processing activity and the purpose.
- The principle of accuracy requires that data must be accurate and, where necessary, kept up to date.
- The principle of storage limitation establishes a very critical and decisive limitation.
- Integrity and confidentiality are main characteristics of the technical and organizational measures, which are constantly mentioned in the Regulation, and concern the security and protection of personal data.
- The regulation also incorporates a new principle, that of accountability. Essentially, it is a summary of the above principles and makes it clear that the data controller is responsible and able to demonstrate compliance with all the previous principles and compliance with the regulation.

3. RIGHTS OF THE DATA PROCESSING SUBJECT

The principle of transparency is interpreted into a series of rights pertaining to physical persons as subjects of data processing. The right of access by the data processing subject, according to Article 15, has a dual nature. Initially, the person receives from the controller information on whether the data is processed and in the event of processing, the person is given the possibility of access own data and to the relevant information regarding the processing thereof.

The right to rectification (Article 16) is governed by the principle of accuracy and is defined in Article 16 of the Regulation. The data subject has the right to require from the controller, without undue delay, the correction of inaccurate or incomplete personal data concerning him/her.

The right to erasure, or the right to be forgotten, is enshrined in Article 17, according to which the data subject has the right to request from the controller the erasure of personal data concerning him or her without undue delay, and the controller is obliged to erase them immediately.

The right to restriction of processing (Article 18) can be exercised by the data subject in cases where the accuracy of his or her data is contested and for the period required by the controller to verify the accuracy of the data, the processing is unlawful, the purposes of the processing are no longer served, but the data subject requires the retention of the data for the establishment, exercise or defense of legal claims and finally, he or she objects to the processing, pending their verification.

The right to portability is a newly introduced concept and is established for the first time in EU law. As set out in Article 20, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and shall have the right to transmit those data to another controller without objection from the controller to whom they were provided. When exercising the right to data portability, the data subject shall have the right to request the direct transmission of the personal data from one controller to another, where technically feasible.

Article 21 enshrines the right to object, according to which the data subject has the right to object, at any time and on grounds relating to his or her particular situation, to the processing of personal data concerning him or her, where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority or for the purposes of the legitimate interests pursued by the controller or by a third party or which are intended for direct marketing purposes.

Right to non-automated individual decision-making, including profiling. As defined in the regulation, "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyze or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is a very common method in big data analytics and used widely for marketing purposes. (Wedel & Kannan, 2016).

4. COMPLIANCE REQUIREMENTS EFFORT

The usefulness and necessity of technical interventions for data protection and privacy were made perfectly understandable and clear throughout the regulation, with the constant references to the phrase "appropriate technical and organizational measures". The term "appropriate" can be interpreted as the measures and guarantees taken must be appropriate in order to achieve the intended purpose. In short, to implement the principles of data protection and privacy in order to effectively serve the rights of the subject. Meaning that appropriateness is inextricably interwoven with the requirement of effectiveness.

To understand what it takes to comply with the regulation, it is necessary to have a look at the technical requirements and protection measures that an organization's IT department is required to implement. The three (3) main axes of the technical and organizational measures concern the protection, governance and access of personal data.

The theory of data protection and privacy by design extends to three dimensions: 1) Information Systems, 2) Business processes, and 3) Physical design and network infrastructure. The intensity of changes required along these three dimensions tends to be proportional to the sensitivity of the data and the risks inherent to specific organizational and IT systems set-ups.

Apart from security and privacy provisions which are necessary to safeguard data protection, GDPR in its core is a data governance exercise. One of the many definitions of data governance is "a companywide framework for assigning decision-related rights and duties in order to be able to adequately handle data as a company asset" (Otto, 2011). Data governance reflects ensuring that data is treated as a strategic asset and that it is managed in a way that supports the organization's goals and objectives. This includes understanding how data is created, captured, stored and used, and implementing processes that ensure data is managed effectively throughout its lifecycle. Effective governance can help organizations improve decision-making, reduce costs and mitigate risks related to data privacy and security. It is easy to conclude that data governance and the regulation are closely related concepts that complement each other. On the one hand, data governance provides the framework for organizations to manage their data as assets in a way that protects the privacy and security of individuals, while on the other hand, the regulation sets out specific requirements for how organizations must protect personal data. In essence, "the regulation requires companies to build a dedicated data management capability" (Labadie & Legner, 2019). Therefore, organizations lacking a mature design and adoption of a data governance framework had to pay a significant price in order to bridge the gap. Data governance contributes significantly to compliance with regulatory requirements that are imposed, such as obtaining and managing consent, the requirement that the organization respond to data subjects' requests based on their rights, the collection, storage and processing of data, as well as the requirement to maintain accurate records of data processing activities. By establishing policies and procedures for data management, organizations can ensure that they have the necessary infrastructure and processes in place to meet these requirements.

The following table tries to interpret the main regulatory principles and mandates into compliance requirements and their resulting high level technical specifications:

No.	GDPR Article	Requirement	Technical specification
5.1	Purpose limitation	Data must be collected and used for specified purposes	Metadata indexing
5.1	Storage limitation	Data must not be stored beyond its purpose	Timely deletion
5.2	Accountability	The controller must be able to demonstrate compliance	Incident management and regulatory reposting
13	Conditions for data collection	Obtain the person's consent on how their data is managed	Event driven information on person's actions regarding information and consent for personal data processing
15	Users' right of access	Give persons timely access to their data	Metadata indexing and specific user interfaces
17	Right to be forgotten	Find and delete sets of data	Identify all data- and work- flows that relate to the specific person

20	Right to data portability	Transfer data to other controllers upon request	Metadata indexing and data dictionary entries
21	Right to object	Data should not be used for purposes that are contrary to the will of the person	Metadata indexing. Ability to support exclusions from data sets in data- and work-flows
25	Protection by design and by default	Securing and limiting access to data; security embedded during design and not afterwards	Threat analysis to drive security design before code development. Access control, encryption, data masking
30	Records of processing activity	Storing audit logs of all operations	Logging and analysis of logs; on-line /off-line monitoring
32	Data security	Implementing appropriate data security measures	Provisions for confidentiality, integrity and availability. Preventive mechanisms
33, 34	Data breach notification	Information and audit trails from relevant systems	Data forensics tools and techniques
46	Transfers subject to safeguards	Terms and conditions for transferring personal data to a third country or an international organization.	Assignment and management of location attributes to data (from/to)

This indicative list of effort required to comply with the regulation demonstrates a pretty good idea of the complexity and the costs incurred to the "GDPR project". The implementation of the compliance specifications represents an opportunity cost for the organization, since this money could be alternatively invested to ensure corporate growth and success. In the next section, the paper presents real world scenarios in which the opportunity cost for GDPR compliance was minimized, since the involved organizations managed to reap the benefits of opportunities opened to them, during the course of actions needed for GDPR compliance.

5. INTERVIEWS AND ANALYSIS OF OPPORTUNITIES

Compliance to this regulation required the implementation of several big IT projects as shown above. Some of them had profound impact on how organizations design, manage, operate and govern information systems. This impact created the conditions for opportunities identification and accrual of benefits for organizations that could manage the change effectively. To reveal these opportunities, four interviews were designed and run, with key persons in three different economy sectors. In the following, a summary of the main points of each interview is provided, focusing on the different opportunities aimed by those four organizations.

The first interview with a banking executive was not a surprise. Banks have been heavily regulated organizations ever since and the emphasis on data and security resides in their DNA. Moreover, they were not unfamiliar their IT governance systems as well as audit practices. Therefore, it seemed that banks were better positioned than any other sector of the economy to comply faster with the regulation. Integrity and confidentiality of information were taken for granted. Nonetheless, the interview with the bank executive revealed that they had to deal with data governance much deeper than before. First of all, data had to be categorized as personal and sensitive personal ones. All applications had to be scrutinized in order to ensure the usage of those data to a bare minimum and that access is granted depending on the needs of the role of the person requesting them. Then, business analysts were helping software applications' asset managers and product / process owners to re-examine the data from the principle of data minimization viewpoint. To comply with the regulation's requirements, the data governance unit had to extend significantly the scope of its work and find answers to questions regarding each and every piece of corporate data with relation to access rights in conjunction to job description, data retention, authority to erase or change the data etc. At that time, some banks had to establish new roles in their organizations, such as data owner, data custodian, etc. that were related to data governance policies and procedures. Thus, GDPG compliance gave the chance to banking organizations to extend their knowledge and practice of data governance to an unpreceded degree, reaping the benefits of unique definitions of data, aligning of data usage across multiple information systems and extracting more value from data, using big data analytics.

To demonstrate compliance, new reports and documentation had to be produced, paving the way for a new breed of information systems, called regulatory information systems, or regutech. In these systems, internal compliance criteria, incident management and reporting as well as documentation for compliance auditing purposes were effectively stored and processed. "A company has to demonstrate a documented audit trail to be in compliance and to further demonstrate how an organization plans to sustain that compliance." (Selig, 2016) To comply with the accountability principle, explained above, a "RegTech approach to GDPR compliance can facilitate an organization meeting its accountability obligations", as research has shown.

(Ryan et. al., 2020) There is more room for research in this area, since it has been acknowledged that "further investigation is needed to understand the implications of emerging technologies on GDPR compliance" (Smirnova & Travieso-Morales, 2024). Overall, the main emphasis in this interview in the banking sector was given to the adoption of data governance theory and practice to its full extend, as a necessary step towards compliance. Also, the executive depicted GDPR compliance as an excellent opportunity to enter to the world of regutech and starting exploring them towards several regulatory reporting requirements.

The second interview was held with an executive from the retail sector. The retail sector was not so much oriented to security issues, therefore the main emphasis here was the investments to protect data stored and processed into their information systems. Security by design and data breach identification, management and reporting had not been in the culture of retail organizations. Even though the retail sector had employed all the necessary security systems due to their electronic shops business, they were not actively pursuing continuous enhancement of their security practices, nor did monitoring the security audit trails that could help resolving a case, had a security breach burst out. As expected, our interviewee commented on the various levels of compliance challenges faced by retail organizations of difference size and structure, agreeing with a previous research finding saying that "SMEs with less focus on data protection struggled to make what they felt was a satisfactory attempt at compliance." (Sirur et. al. 2018) Declaring compliance is one thing; another is to demonstrate that organizations have the ability to implement in a non-error prone, systematic way the basic data processing subject rights presented above, as bestowed to them by the regulation. To this end, retail organizations have designed new business processes to ensure that these rights can be exerted to their full extent. "Businesses must also ensure that the processes designed during the preparations for the GDPR actually work and produce the expected results. Areas of particular concern include enabling the rights of data subjects, handling breaches and crises, and managing audit processes." (Mikkelsen et. al, 2019) Apart from implementing new information systems functionalities, organizational maturity with regard to new procedure adoption has been of paramount importance to sustain compliance and provide the necessary evidence.

Executives from utility organizations (energy, telecoms) were the last two interviews. It was interesting to talk to people working in companies that are employing push marketing techniques, therefore they use a lot personal data of their customers as well as for prospects. In both interviews it was made clear that mapping their data flows was their main concern. Due to a very fast growth rate over the last two decades prior to GDPR regulation emergence, detailed documentation of business processes and procedures was not a topic of focus as compared to the need to open up the market and gain a better market share. Therefore, these organizations started immediately a demanding exercise to map their data flows using business process analysts and data flow mapping tools. This exercise led early enough to the identification of areas with great potential for business process re-engineering. Moreover, the acquired knowledge opened up the way towards information systems interconnection of formerly disparate applications using robotic process automation (RPA) to substitute error-prone, tedious manual work. RPA has been identified as a key enabler of digital transformation for organizations (Rizk et. al., 2020) Using low code-no code platforms and armed with the new business process redesigns, these organizations "discovered" the brave new world of empowering their customers and prospects to initiate and complete several customer facing transactions over web interfaces, so as customer on-boarding, know-your-customer type of transactions, etc. Starting from data flow mapping, they exploited the opportunity to design new digital customer journeys (Følstad and Kvale, 2018) which led slowly but firmly, to their digital transformation. It is, thus, fair to infer that digital transformation was indeed accelerated by actions required to achieve compliance with the GDPR regulation.

6. CONCLUSIONS

It has become apparent from those four interviews that GRPD compliance gave the opportunity to learning organizations to identify their weaknesses, reinforce their strengths, reveal opportunities and pay attention to their threats with regard to data processing and business process design. Through the various activities carried out during the GDPR compliance project, organizations revisited and re-evaluated their information governance structure and practice as well as the effectiveness of their enterprise architecture management, both of which have been proved as enablers of GDPR compliance (Zaguir et. al., 2024). Several research papers have shed some light on the impact of GDPR compliance on organizations e.g. (Machado et. al., 2023), challenges and enablers to implementation, e.g. (Daoudagh & Marchetti, 2022), (Tsaneva, 2019), (Dode, 2018), (Kutyłowski et. al., 2020) as well as the costs of compliance (Chander et. al., 2021). This study, based on a qualitative analysis of interviews with executives from three different economy sectors, presented how the burden of compliance was turned into an opportunity for acquiring new organizational capabilities far outreaching the benefits of mere compliance.

Our study has documented through real-word cases, as described in the analyzed interviews, the claim made by another research that "under some market conditions, the GDPR has unintended and so far unrecognized effects on competition, efficiency, innovation, and the resultant welfare." (Gal and Aviv, 2020) Although regulatory compliance may have implications that are far reaching within organizations, it has not yet been given the appropriate attention as a factor of corporate growth and organizational maturity. For example, regulatory compliance has not been identified among the enablers of information technology governance proposed by the COBIT framework in conjunction with a systematic literature review (Henriques et.

al., 2020) Using material from four interviews in three main sectors of the economy, opportunities for enhanced IT governance and digital transformation capabilities through GDPR compliance were clearly evidenced. This study is useful in identifying the opportunities opened to organizations that used GDPR compliance as a learning path towards increased organizational maturity and operational efficiency and effectiveness.

REFERENCES

1. Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving privacy: costs of compliance and enforcement of data protection regulation. Georgetown Law Faculty Publications and Other Works. 2374. Policy Research Working Paper 9594. World Bank's World Development Report 2021 Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. Available at: https://scholarship.law.georgetown.edu/facpub/2374
2. Daoudagh, S., & Marchetti, E. (2022). The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities. In ICISSP (pp. 571-578).
3. Dode, A. (2018). The challenges of implementing general data protection law (GDPR). In 14th International Conference "Standardization, Protypes and Quality: A Means of Balkan Countries' collaboration (p. 65).
4. Følstad, A., and Kvale, K. (2018). Customer Journeys: A Systematic Literature Review. Journal of Service Theory and Practice (28:2), pp. 196–227. (https://doi.org/10.1108/JSTP-11-2014-0261).
5. Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. Journal of Competition Law & Economics, 16(3), 349-391.
6. Henriques D., Pereira R., Almeida R.,Mira da Silva M. (2020) IT Governance Enablers. Foresight and STI Governance, vol. 14, no 1, pp. 48–59. DOI: 10.17323/2500-2597.2020.1.48.59
7. Kutyłowski, M., Lauks-Dutka, A., & Yung, M. (2020). Gdpr–challenges for reconciling legal rules with technical reality. In Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25 (pp. 736-755). Springer International Publishing.
8. Layton, R., & Elaluf-Calderwood, S. (2019). A social economic analysis of the impact of GDPR on security and privacy practices. In 2019 12th CMI Conference on Cybersecurity and Privacy (CMI) (pp. 1-6). IEEE.
9. Labadie, C., & Legner, C. (2019). Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. In Proceedings of the 14th International Conference on Wirtschaftsinformatik.
10. Machado, P., Vilela, J., Peixoto, M., & Silva, C. (2023, May). A systematic study on the impact of GDPR compliance on Organizations. In Proceedings of the XIX Brazilian Symposium on Information Systems (pp. 435-442).
11. Mikkelsen, D., Soller, H., Strandell-Jansson, M., & Wahlers, M. (2019). GDPR compliance since May 2018: a continuing challenge. McKinsey & Company, 22.
12. Otto, B. (2011). Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. Communications of the AIS, 29, 45–66.
13. Rizk Y, Isahagian V, Boag S, Khazaeni Y, Unuvar M, Muthusamy V, et al. (2020) A Conversational Digital Assistant for Intelligent Process Automation. International Conference on Business Process Management, pp. 85-100.
14. Ryan, P., Crane, M., & Brennan, R. (2020). Design challenges for GDPR RegTech. arXiv preprint arXiv:2005.12138.
15. Selig, G. J. (2016). IT governance-an integrated framework and roadmap: How to plan, deploy and sustain for improved effectiveness. Journal of International Technology and Information Management, 25(1), 4.
16. Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd international workshop on multimedia privacy and security (pp. 88-95).
17. Smirnova, Y., & Travieso-Morales, V. (2024). Understanding challenges of GDPR implementation in business enterprises: a systematic literature review. International Journal of Law and Management, 66(3), 326-344.
18. Sustain for Improved Effectiveness," Journal of International Technology and Information Management:
19. Talens, A. C. (2024). Assessing the Economic Effects of GDPR Compliance on European Businesses. Economic Review of the European Union, 7(2), 24-52.
20. Tsaneva, M. (2019). Challenges of GDPR compliance in consumer financing companies. In Conferences of the department Informatics (No. 1, pp. 103-115). Varna: Publishing house Science and Economics Varna. 25(1), Article 4. Available at: https://scholarworks.lib.csusb.edu/jitim/vol25/iss1/4
21. Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. Journal of marketing, 80(6), 97-121.