A Framework for Investigating GDPR Compliance Through the Lens of Security

Angelica Marotta[1](✉) and Stuart Madnick[2]

[1] MIT Sloan School of Management, 245 First Street, Cambridge, MA 02142, USA
amarotta@mit.edu

[2] MIT Sloan School of Management, 100 Main Street, Cambridge, MA 02142, USA
smadnick@mit.edu

Abstract. The General Data Protection Regulation (GDPR) was widely seen as a significant step towards enhancing data protection and privacy. Unlike previous legislation, adherence to GDPR required organizations to assume greater responsibility for cybersecurity with respect to data processing. This shift represented a profound transformation in how businesses retain, use, manage, and protect data. However, despite these innovative aspects, the actual implementation of the GDPR security side poses some challenges. This paper attempts to identify positive and negative aspects of GDPR requirements and presents a new framework for analyzing them from a security point of view. Firstly, it provides an overview of the most significant scholarly perspectives on GDPR and cybersecurity. Secondly, it presents a systematic roadmap analysis and discussion of the requirements of GDPR in relation to cybersecurity. Results show that some of the GDPR security controls, such as the Data Protection Impact Assessments (DPIA), records on processing, and the appointment of a Data Protection Officer (DPO), are some of the most critical from a security viewpoint. Finally, it provides recommendations for tackling these challenges in the evolving compliance landscape.

Keywords: GDPR · Cybersecurity · Compliance · Regulations · Risk management

1 Introduction

Today, every organization has a "digital footprint." Every time employees communicate, engage with customers through the Internet, use a device, or simply advertise their business, they are leaving a data trail behind them. The more data they share, the more their digital footprint grows. With the large volume of information that must be handled, it is challenging to keep track of which digital assets need to be secured. As a result, data protection is now a major area of focus in the field of compliance and security. The introduction of the General Data Protection Regulation (GDPR), which came into effect in the European Union on 25 May 2018, was widely seen as a significant step towards enhancing data protection and privacy [1]. The Regulation was designed to allow individuals to control their data and require organizations to better handle data processing.

J. Bentahar et al. (Eds.): MobiWIS 2021, LNCS 12814, pp. 16–31, 2021.
https://doi.org/10.1007/978-3-030-83164-6_2

Individuals and regulators were presented with new regulatory mechanisms, including administrative fines and an extension of the requirements' scope. In this context, the new security requirements under the GDPR benefitted from the lessons learned from data protection authorities' past experience and a more conscious conception of the digital environment in which companies operate. The GDPR specifically explains what risks data processing may pose, such as identity fraud, professional secrecy issues, data disclosure, etc. Figure 1 shows the main security aims of the GDPR [2].

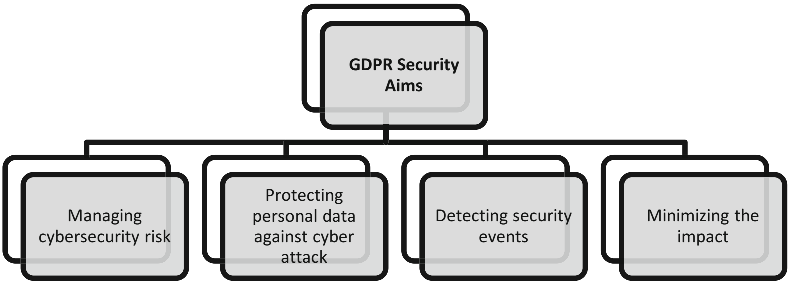
GDPR Security Aims
Managing cybersecurity risk
Protecting personal data against cyber attack
Detecting security events
Minimizing the impact

Fig. 1. GDPR security aims

However, despite these innovative aspects, there is some confusion regarding the actual implementation of the GDPR's security side. Some argue that GDPR provides a solid security structure to operate by, but the reality is more complicated. GDPR is primarily data privacy legislation whose main pillars are privacy, policy, and cybersecurity. Organizations need to implement all three pillars to successfully comply with the strict requirements of the GDPR and be secure. Marotta and Madnick [3–5] investigated this issue in an extensive way. In particular, the authors argue that compliance is not black and white but rather a combination of factors, which may either have a positive or negative impact on cybersecurity. In this paper, this concept is further extended to explore the impact of GDPR "through the sense of security." More specifically, the study examines each GDPR requirement with particular attention to security to identify controls that are likely to increase or reduce the general level of cybersecurity in an organization. The work provides the following contributions to the study of cybersecurity compliance. Firstly, it offers a review of the main scholarly viewpoints on GDPR and cybersecurity. Secondly, it presents a systematic analysis and discussion of the requirements of GDPR with respect to cybersecurity. Thirdly, it provides recommendations and future perspectives on the evolving compliance landscape.

2 Literature Review and Background

In today's changing threat landscape, businesses are required to perform two essential and intertwined tasks: proactively addressing cyber risks and maintaining compliance with laws and regulations. However, as shown in the comparative compliance analysis conducted in a previous study [6], several issues prevent companies from pursuing these objectives and achieving an effective balance between compliance and cybersecurity.

Some of them depend on the industry in which a company operates. For example, in the healthcare sector, regulatory language may make it difficult for health operators and patients to comprehend and interpret regulations. These considerations apply to almost every enforcement setting, but they are particularly pertinent in the context of GDPR [7]. For example, Huth and Matthes (2019) argued that GDPR poses challenges regarding the integration of privacy concerns in software development processes. Tsohou et al. [8] also agreed that data controllers face difficulties complying with the GDPR and proposed mechanisms and tools to assist organizations in adhering to the requirement. Conversely, other authors who conducted analyses on this topic found positive results [9]. For example, Horák et al. [10] discussed the impact of GDPR on cyber-security software and operations. In particular, they conducted a DPIA assessment to investigate risks related to information sharing in cybersecurity. Their findings indicated that the risks were not high and that the DPIA aided in a better understanding of risks and their management. They also pointed out that this assessment provides a solid ground for information sharing in cybersecurity under GDPR. Along with this line of thought, Lachaud [11] argued that the GDPR (particularly Article 42 and 43) "encourages data controllers and processors to use third-party certification schemes to voluntarily demonstrate their conformity with the GDPR." According to the author, this "endorsement" represents a new type of "regulation instrument" whose flexibility helps fill the gap between self-regulation and regulation. Another research trend observed in the literature is the use of comparative analysis to investigate whether the security principles outlined in the GDPR are consistent with other frameworks. Saqib et al. [12] performed a comparison between the security requirements of the GDPR and the Directive on security of network and information systems (NISD). More specifically, the author studied how GDPR influences the NISD. This mapping provided interesting results regarding possible difficulties that businesses may experience while implementing compliance with GDPR and NISD. Other scholars conducted a similar investigation to compare the controls provisioned in ISO standards (e.g., ISO/IEC 27001:2013 and ISO/IEC 27002:2013) and the data protection requirements set by the GDPR [13–15]. These studies agree in assessing the importance of integrating GDPR with other frameworks and evaluating multiple factors that have an impact on security.

2.1 Brexit and the UK Version of GDPR

According to Marotta and Madnick [6] an essential factor influencing the relationship between compliance and security is the geographical aspect surrounding compliance. According to the authors [6], "regulations uniquely impact organizations and the global actors connected to their operations." As shown in a case study[1] conducted by the same authors [6], this aspect is particularly evident in Europe due to the high level of interdependencies among the Member States. For example, according to Chivot and Castro [16], the European Commission stated that one year after the introduction of the GDPR, some Member States, such as Greece, Portugal, and Slovenia, still had not completely adopted national legislation to adhere to the GDPR. Therefore, Member

[1] Case Study #5: Understanding the Compliance Forces that Influence Cybersecurity in the Banking Sector, especially in the UK.

States struggled to homogeneously implement the Regulation across Europe. Following Brexit (the UK's exit from the EU), this issue became more pronounced because the UK is no longer regulated domestically by the GDPR. Instead, the UK now has incorporated the GDPR into its data protection law; it created its own version (known as the UK-GDPR), which took effect on 31 January 2020 [17]. UK organizations are now required to amend their GDPR documentation to align it with the new regulatory criteria. The UK-GDPR security aims remained conceptually the same (outlined above in Fig. 1) [2]. However, in the context of the UK-GDPR, these aims need to be adapted to the new scope of the Regulation and reflect the independent jurisdiction of the UK. To make this transition easier, the EU established a period of six months (lasting until June 2021) to ensure the unrestricted flow of data between the UK and the EU. Nevertheless, for some companies, this transitional phase means that there are still two different GDPR laws they have to deal with – one that applies if they have users from inside the EU, the other if they have users from inside the UK. This situation further complicates the processing of data and the consequent security implications.

3 Analysis of GDPR Requirements

The GDPR is intended to protect EU citizens from privacy or data breaches [1]. A personal data breach can be generally defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In the context of GDPR [1], a personal data breach is defined in Article 4(12) as:

> *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

This definition comprehensively describes a security breach; it shows the descriptive nature of the Regulation. Although the GDPR requires an analysis of the organizations' data processing activities and an evaluation of the necessary control measures, it is not intended to prescribe which requirements controllers are required to undertake. Its focus is on EU citizens' rights in relation to their personal data, and data security is just one aspect of that. Unlike other regulations, such as Payment Card Industry – Data Security Standard (PCI-DSS) and other standards with a specific list of security requirements, the GDPR covers security only at a very high-level. Thus, the GDPR gives companies the freedom to develop and define their control measures and meet their security goals. However, with greater flexibility comes greater responsibility which often many organizations tend to underestimate. This factor means that implementing the controls outlined by the GDPR does not guarantee that organizations are fully safeguarded from cyber-attacks or that an employee does not mistakenly or purposefully disclose confidential data. The following analysis shows the positive and negative effects of the descriptive nature of GDPR.

3.1 Framework for Cybersecurity Compliance

The GDPR is divided into 99 Articles (and 173 Recitals). These Articles regulate the GDPR requirements that must be followed to be compliant and are explicit in terms of what is required from enterprises in relation to the collection and management of personal data. Subsections of the Articles are divided into Paragraphs, which are, in turn, divided into Points. Articles and Paragraphs are numbered sequentially throughout the Regulation document, while Points are sorted alphabetically. Paragraphs and Points of the Articles contain all explanatory notes of the Articles. Table 1 maps the main requirements (identified by the corresponding Articles, Paragraphs, and Points) that directly influence the implementation of security. For each of them, it provides an evaluation of the related security goals and compliance elements that may help (advantages) or hinders (disadvantages) the development of efficient cybersecurity strategies.

This analysis was performed through the *mapping methodology*[2] to identify the associations between compliance requirements and security impacts (each requirement of GDPR mentioned has both a positive and a negative aspect) [18]. Each requirement was also put in relation with its ideal security goal[3]. The included requirements were used to develop a greater understanding of security concepts and identify evidence for compliance-relevant issues and gaps. The resulting elements of this analysis are explained in the section below.

4 Discussion of Results

Table 1 revealed that GDPR introduced several security controls that potentially provide both advantages and disadvantages in relation to the initial security goal established by the GDPR. However, the degree to which a requirement is more or less advantageous (or disadvantageous) from a cybersecurity viewpoint is given by the relationship between the level of relevance attributed by the GDPR to a specific requirement in terms of security (indicated as "security goal" in Table 1) and the actual impact of that requirement on the overall organizational cybersecurity infrastructure[4]. Table 2 shows the values of these two variables[5] for each requirement (Articles).

The values indicated in Table 2 are visually presented in Fig. 2. The left-right (horizontal) direction represents the level of relevance of the security goal for a requirement; the up-down (vertical) direction represents the actual impact of the requirement. The correspondence between impact and relevance determines whether a requirement (Article) is advantageous or disadvantageous in terms of security. Articles located above the diagonal line are considered disadvantageous, while those located below the diagonal line are considered advantageous. All Articles located on the diagonal line are equally advantageous and disadvantageous.

Results show that the most critical security area of GDPR is that concerning security controls in relation to data protection (defined in the Regulation as "security of

[2] The mapping methodology is a research-based method for recording qualitative information, analyzing its distribution, and prioritizing relevant information in relation to a specific topic or research issue.

[3] The desirable compliance goal of a GDPR requirement established by the Regulation.

[4] Real impact of a GDPR requirement on cybersecurity practices, processes, and behaviors in an organization.

[5] The variables can assume the following values: Low = 1, Medium = 2, High = 3, Very High = 4.

Table 1. GDPR compliance framework

Article	Paragraph	Point	Requirement	Security goal	Advantages	Disadvantages
5 - Principles relating to processing of personal data	1	(f)	"…data shall be processed in a manner that ensures appropriate security of the personal data…"	Integrate security into personal data processing	Flexibility in forming cybersecurity programs	High level of uncertainty for organizations
	2	–	"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."	Keep the controller (organization) accountable for security	Increase detection of bad behaviors, and customer trust	Employee liability is not covered
24 - Responsibility of the controller	1	–	"… the controller shall implement appropriate technical and organisational measures…"	Establish transparency over security procedures	Ensure the existence of data protection policies procedures	It does not provide an exhaustive list of all the obligations of the controller
25 - Data protection by design and by default	2	–	"…such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."	Limit data availability	Ensure that personal data access is restricted to selected users	Hard to define the scope of data access

(*continued*)

Table 1. (*continued*)

Article	Paragraph	Point	Requirement	Security goal	Advantages	Disadvantages
30 - Records of processing activities	1	–	"Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility"	Ensure data availability for controllers	Reduce data storage costs and keep security information organized	No guidance on how to securely store information
32 - Security of processing	1	(a)	"…pseudonymisation and encryption of personal data."	Implement data protection by design	Increase security of data	Abstract and insufficient ways to protect data (e.g. the use of encryption)
		(b)	"ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"	Implement the CIA Triad	Ensure basic security goals	Provide broad, generic framework
		(c)	"…ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	Restore the availability	Greater trust between data subjects and organizations	Lack of guidance regarding restoring measures

(*continued*)

Table 1. (*continued*)

Article	Paragraph	Point	Requirement	Security goal	Advantages	Disadvantages
		(d)	"…process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."	Test and evaluate the effectiveness of security measures	Minimize the risk of a data breach and protect reputation	Lack of specification regarding the frequency
	2		"In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing…"	Consider security risks in the data processing	Make security an integral part of organizational procedures	Subjective risk-based approach to security
33 - Notification of a personal data breach to the supervisory authority	1		"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 h after having become aware of it, notify the personal data breach to the supervisory authority competent "	Report breaches	Promote incentives to strengthen data security	Subjective judgement of whether or not the breach represents an actual risk

(*continued*)

Table 1. (*continued*)

Article	Paragraph	Point	Requirement	Security goal	Advantages	Disadvantages
	3	(d)	"…. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."	Document reporting procedures	Encourage mitigation measures and reflection on the efforts taken to mitigate the attacks	The requirement is vague about definition of "measures"
35 - Data protection impact assessment	1	–	"…the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data…"	Identify and minimize risks resulting from data processing	Lower likelihood of data breach events	The context in which the DPIA is carried out is not strictly defined
37 - Designation of the data protection officer	1	–	"…The controller and the processor shall designate a data protection office…"	Provide general consultancy on security-related matters	Maintain an adequate security level across the organization	Delay internal security procedures

Table 2. Values of impact and security relevance

Article	Paragraph	Point	Cybersecurity impact	Relevance of security goal
5 - Principles relating to processing of personal data	1	(f)	3	4
	2	–	3	1
24 - Responsibility of the controller	1	–	4	1
25 - Data protection by design and by default	2	–	4	2
30 - Records of processing activities	1	–	4	2
32 - Security of processing	1	(a) - (d)	4	4
	2	–	3	4
33 - Notification of a personal data breach to the supervisory authority	1	–	2	4
35 - Data protection impact assessment	2	–	2	3
	1	–	4	3
37 – Designation of the data protection officer	1	–	1	1

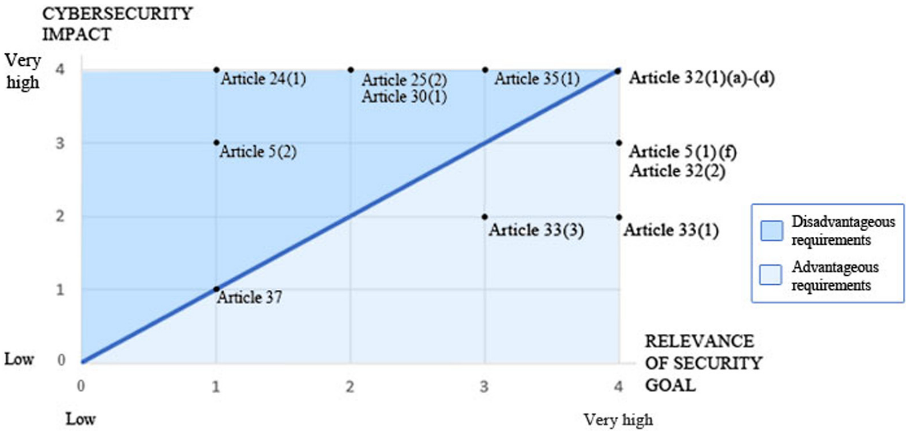

Fig. 2. Advantages and disadvantages of GDPR compliance

processing"). Such controls are addressed in the GDPR in the form of technical and organizational measures (Article 24 and 32, data protection impact assessments (DPIAs) (Article 35), records on processing (Article 30), data protection by design and by default techniques (Article 25) and the appointment of a Data Protection Officer (DPO) (Article 37). More advantageous controls appear in the GDPR's Article 5(1)(f),

> "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*"

The objective of this requirement is to ensure that personal data processing is performed considering integrity and confidentiality. However, not all organizations require the same degree of cybersecurity protection, which is why regulators purposefully left this requirement vague. On the one hand, this openness enables organizations to form their cybersecurity programs in a flexible manner; on the other hand, it leaves them with uncertainty about how to process data in "a manner that ensures appropriate security." The previously mentioned controls are also characterized by a certain degree of generality. The introduction of the DPIA as a means to identify high risks in relation to data processing is defined in a way that does not provide a clear picture of the procedure's contents. Some organizations already perform similar assessments (e.g., PIAs), and having a more accurate description of what DPIAs involve could help them get more uniform assessments. Article 5(2) is a requirement that has a significant impact on cybersecurity, although not directly (low level of security relevance from the standpoint of GDPR). It requires data controllers (in this context, "data controller" does not refer to one single individual within an organization but to the organization itself) to be responsible for and be able to demonstrate compliance with the GDPR's data protection principles defined in paragraph 1:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality security

In addition to the six data protection principles, the Regulation introduces the principle of *accountability* in Article 5(2) itself[6]. This principle has two facets: being responsible for compliance and being able to demonstrate compliance. However, the Regulation specifies that the responsibility to demonstrate compliance with this principle rests with the controller [1]. While this aspect is a fundamental part of an effective cybersecurity program, it may limit the scope of security responsibility of those involved in data processing security. Therefore, if an organization acts as the controller of its customers' data and employs inadequate security measures that result in unauthorized data access, the

[6] The GDPR ensures the implementation of three principles of the "CIA triad" (confidentiality, integrity, and availability).

organization is subject to GDPR penalties. However, the organization's cybersecurity manager responsible for guaranteeing personal data security would not have any types of regulatory "punishments." Another stakeholder who has no direct accountability for security is the DPO (Article 37). However, this regulatory figure has a significant role in implementing the Regulation and the consequent maintenance of an adequate security level. According to an October 2018 survey, a majority of companies (52%) that have appointed a DPO said they established one for compliance reasons only, and that the role did generate business benefits, including better security [19]. The DPO is an expert who has a predominantly legal profile, although he or she possesses some expertise in IT and risk management[7]. Its primary function is to provide supervision, evaluation, and regulatory consultancy regarding personal data processing management within a company. This professional figure is one of the first to be consulted when a data breach or other incident occurs. Apart from this instance, the GDPR does not indicate when consultation with the DPO is necessary or at least recommended. The lack of guidance regarding this aspect may delay internal security procedures or lead organizations to considering the DPO's role irrelevant. Furthermore, while the DPO is supposedly prepared enough to interact and communicate effectively with cybersecurity, the limitation of expertise on the topic can lead to decision-making issues. These characteristics make this requirement equally advantageous and disadvantageous from a security perspective (although not particularly determinant). Technical and organizational measures are further explained in Article 32, which requires implementing "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." For example, a well-balanced requirement is Article 32 (1), which mandates the assessment of the security of processing, which also must consider "the state of art." The use of this very generic word is presumably a deliberate decision of regulators, which may be based on lessons learned from past experiences. The advantage of having "open" formulations is providing flexibility to the law and permitting its adaptation to different contexts and cases. Additionally, considering the rapid development of technology, it would prevent organizations from implementing outdated measures. However, in the absence of a more restrictive rule, organizations need to refer to common practice or other frameworks to perform security analyses and assess risk. Article 32, therefore, limits cybersecurity programs to a subjective risk-based approach to security, which may leave room for inaccurate interpretations. Finally, one controversial requirement of the GDPR is Article 33(1) that provides that, "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 h after having become aware of it, notify the personal data breach to the supervisory authority." Article 33 also specifies that if the organization can establish that the breach did not cause risks[8] for the data subjects or other individuals, then it has no obligations. The introduction of this rule (a new requirement under the GDPR) has positively impacted cybersecurity by emphasizing the focus on detection and reporting of cybersecurity incidents. One of

[7] According to Article 39, the DPO "shall in the performance of his or her tasks have due regard to the risk associated with processing operations," including security risk.

[8] For example, loss of sensitive personal data, such as medical records, email address, IP address or images.

the most immediate benefits of this obligation is the increased proactiveness; organizations are incentivized to protect both customers and the brand's reputation. A study performed by Neto et al. [20] compared reporting statistics in Europe and North America in a period between 2018 and 2019. They found that the number of reported attacks in North America increased by 38%, but by 80% in Europe, which is likely the consequence of the introduction of the GDPR. This output has also been formulated by the UK's independent authority (ICO). According to the ICO, the number of reports from all data controllers quadrupled following this requirement's implementation. However, the ICO also observed that more than 82% of the reported data breaches required no action from the organization [21]. Organizations are obliged to disclose personal data breaches to data protection authorities, but the way they manage their implications is subjective. This aspect leaves room for negligence, resulting in issues not being properly handled. In light of these considerations, it is clear that GDPR has a twofold effect on cybersecurity. On the one hand, it is important to note that it encourages organizations to have some form of cybersecurity strategy. The GDPR provides the opportunity to implement new or updated data protection and cybersecurity policies, processes, practices, and technical controls, including measures to secure data and data processing procedures. On the other hand, the analysis suggests that organizations may also report negative impacts because of the GDPR. For example, organizations may need to invest significantly in measures that are not sufficient to ensure security, including encryption. Subjectivity is also another negative factor, which may lead organizations to losing control over their cybersecurity goals. Therefore, while GDPR may provide an incentive and a guarantee for companies to strengthen data security, it is not intended to create an explicit duty to protect data, leaving companies vulnerable. As a result, the most considerable risk of GDPR is focusing excessively on the protection of data to the detriment of cybersecurity aspects. This swings the balance toward the assumption that GDPR might not be a key cybersecurity catalyst for organizations. However, an in-depth analysis of this hypothesis might be necessary to determine which aspects dominate in real-life settings and under what circumstances.

5 Recommendations and Future Perspectives

The inherent subjectivity of GDPR provides an interesting perspective to consider when evaluating GDPR requirements in terms of security. Despite having appropriate security measures in place and reporting breaches when necessary under the GDPR, an organization may still fail from a security point of view. It is, therefore, essential to be mindful of the main security goal of the GDPR, which is not to prevent data breaches but to ensure an appropriate security level. As a result, businesses are forced to plan for various situations. Some have also established GDPR task forces in the event that initial compliance decisions produce a different interpretation of the Regulation.

5.1 Recommendations: Organizational and International Contexts.

The organization's IT side needs to have an active role in advising the rest of the organization on what measures (both technical and organizational) are appropriate to minimize the risk of data breaches. For example, an organization may need assistance in implementing disaster recovery and business continuity plans and ensuring that the control measures remain in place and are effective [22]. In particular, the essential areas where the IT team can assist with GDPR compliance include those related to the requirements that are considered “disadvantageous” in Fig. 2 (e.g., accountability, data retention, DPIAs, and breach containment). From an international perspective, IT teams can also assist in determining whether and how data are being transferred to territories outside of the Economic European Area (EEA). However, to get the right and most relevant guidance towards security requirements, everyone in the company must take responsibility for keeping data handling activities secure and communicating with the IT team.

5.2 Future Perspectives

The first years of the GDPR were not as expected, but it is also true that a lot has happened since the GDPR’s introduction. When the GDPR came into force in 2018, the world could never have foreseen the security complexities and implications of Brexit or the unprecedented Coronavirus pandemic. Consequently, there has been a greater emphasis on increasing data protection and has resulted in an enhancement of privacy legislation at a global level. Compliance with global security rules is becoming a larger concern for businesses around the world. The GDPR is not the only EU privacy regulation on policymakers’ and companies’ minds. The ePrivacy Regulation (ePR), intended to replace the 2002 ePrivacy Directive, deserves particular consideration as it is noteworthy in the European context of cybersecurity and the protection of information [23]. Alongside the GDPR, the new privacy regulation is set to introduce harmonized rules on the processing of data by electronic communications service providers (now extended to include WhatsApp and Facebook Messenger). As the GDPR matures and similar regulations take shape, the future of cybersecurity compliance is certainly more encouraging than it has been previously in terms of security. European organizations now have the opportunity to strengthen their data security policies and adapt to GDPR standards in a more targeted way. However, it is also necessary to consider that data protection relies on awareness and proactive measures to handle cybersecurity risks and ensure privacy effectively. Research on cybersecurity compliance has the potential to help in many critical areas related to GDPR security. For example, it is important to develop frameworks and methods to investigate how organizational culture and specific national dynamics influence the implementation and compliance of the GDPR and explore how regulators can improve and simplify the rules related to data processing security.

6 Conclusion

The adoption of GDPR has had a strong effect on privacy and protection practices while implicitly encouraging companies to strengthen and improve their information security policies, thus limiting possible data violations. It has dramatically increased European companies’ understanding of cybercrime data breaches and the need for security. GDPR has given cybersecurity more weight by providing awareness on the concrete implications of cybercrime. However, while steps of progress have been taken in improving cybersecurity through GDPR, it cannot be assumed that the requirements imposed by the legislation are enough to handle cybersecurity in the context of privacy. Following scandals such as Cambridge Analytica and Facebook in recent years, as well as a high number of severe data breaches, concerns about the use and security of data have started to rise [24]. It has, therefore, become clear that the approach to addressing cybersecurity lies as much with mandatory regulatory requirements as it does with integrative measures.

Acknowledgements. The research reported herein was supported in part by the Cybersecurity at MIT Sloan initiative, which is funded by a consortium of organizations, and a gift from C6 bank.

References

1. The European Parliament and the Council of the European Union: 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 (2016)
2. ICO Security outcomes | ICO. In: ico.org.uk. https://ico.org.uk/for-organisations/security-outcomes/. Accessed 25 Mar 2021
3. Madnick, S.E., Marotta, A., Novaes Neto, N., Powers, K.: Research Plan to Analyze the Role of Compliance in Influencing Cybersecurity in Organizations (2020)
4. Marotta, A., Madnick, S.E.: Analyzing the interplay between regulatory compliance and cybersecurity (revised). SSRN Electron. J. (2020). https://doi.org/10.2139/ssrn.3569902
5. Marotta, A., Madnick, S.: Perspectives on the relationship between compliance and cybersecurity. J. Inf. Syst. Secur. **16**, 27 (2021)
6. Marotta, A., Madnick, S.: Issues in information systems convergence and divergence of regulatory compliance and cybersecurity. **22**, 10–50 (2021). https://doi.org/10.48009/1_iis_2021_10-50
7. Zerlang, J.: GDPR: a milestone in convergence for cyber-security and compliance. Netw. Secur. **2017**, 8–11 (2017). https://doi.org/10.1016/S1353-4858(17)30060-0
8. Tsohou, A., Magkos, E., Mouratidis, H., et al.: Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. Inf. Comput. Secur. **28**, 531–553 (2020). https://doi.org/10.1108/ICS-01-2020-0002
9. Poritskiy, N., Oliveira, F., Almeida, F.: The benefits and challenges of general data protection regulation for the information technology sector. Digit. Policy Regul. Gov. **21**, 510–524 (2019). https://doi.org/10.1108/DPRG-05-2019-0039
10. Horák, M., Stupka, V., Husák, M.: GDPR compliance in cybersecurity software: a case study of DPIA in information sharing platform. In: ACM International Conference Proceeding Series, pp. 1–8. Association for Computing Machinery, New York (2019)
11. Lachaud, E.: The General Data Protection Regulation and the rise of certification as a regulatory instrument (2018)
12. Saqib, N., Germanos, V., Zeng, W., Maglaras, L.: Mapping of the security requirements of GDPR and NISD. ICST Trans. Secur. Saf. **166283** (2018). https://doi.org/10.4108/eai.30-6-2020.166283
13. Diamantopoulou, V., Tsohou, A., Karyda, M.: General Data protection regulation and ISO/IEC 27001:2013: synergies of activities towards organisations' compliance. In: Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) TrustBus 2019. LNCS, vol. 11711, pp. 94–109. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27813-7_7

14. Diamantopoulou, V., Tsohou, A., Karyda, M.: From ISO/IEC 27002:2013 information security controls to personal data protection controls: guidelines for GDPR compliance. In: Katsikas, S., et al. (eds.) CyberICPS. LNCS, vol. 11980, pp. 238–257. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-42048-2_16
15. Lopes, I.M., Guarda, T., Oliveira, P.: How ISO 27001 can help achieve GDPR compliance. In: Iberian Conference on Information Systems and Technologies, CISTI. IEEE Computer Society (2019)
16. Chivot, E., Castro, D.: What the Evidence Shows About the Impact of the GDPR After One Year. Cent. DATA Innov (2019). http://www2.datainnovation.org/2019-gdpr-one-year.pdf. Accessed 25 Mar 2021
17. GOV.UK. Data protection - GOV.UK. Gov.uk (2014). https://www.gov.uk/data-protection/the-data-protection-act. Accessed 25 Mar 2021
18. Sutherland, S., Katz, S.: Concept mapping methodology: a catalyst for organizational learning. Eval. Program. Plan. **28**, 257–269 (2005). https://doi.org/10.1016/j.evalprogplan.2005.04.017
19. IAPP, Ernst, Young: IAPP-EY Annual Governance Report 2019 (2019)
20. Neto, N.N., Madnick, S., Paula, A.M.G.D., Borges, N.M.: Developing a global data breach database and the challenges encountered. J. Data Inf. Qual. **13**, 1–33 (2021). https://doi.org/10.1145/3439873
21. ICO. Information Commissioner's Annual Report and Financial Statements. ICO (2019)
22. Marotta, A., Martinelli, F.: GDPR survey: an analysis of the tools used for assessing GDPR compliance. Technical report (IIT B4-05/2020) - IIT CNR (2020)
23. Vinet, L., Zhedanov, A.: A "missing" family of classical orthogonal polynomials (2011)
24. Isaak, J., Hanna, M.J.: User data privacy: Facebook, Cambridge analytica, and privacy protection. Comput. (Long Beach Calif.) **51**, 56–59 (2018). https://doi.org/10.1109/MC.2018.3191268