VNU Journal of Science: Legal Studies

Journal homepage: https://js.vnu.edu.vn/LS

Original Article

Enhancing the Responsibilities of Data Controllers in Vietnam: Insights from the European General Data Protection Regulation

Dao Kim Anh[1,*], Pham Xuan Phong[1], Phan Duong Quang[2]

[1]*Foreign Trade University, 91 Chua Lang, Dong Da, Hanoi, Vietnam*

[2]*Diplomatic Academy of Vietnam, 69 Chua Lang, Dong Da, Hanoi, Vietnam*

Received 11 January 2024
Revised 26 February 2024; Accepted 20 March 2024

Abstract: This article explores the evolving landscape of data protection law in Vietnam, focusing specifically on the responsibilities of data controllers under Vietnam's new Personal Data Protection Decree (Decree No. 13/2023/ND-CP - hereinafter referred to as Decree 13) and compares it with the European Union's General Data Protection Regulation (GDPR). The main objective is to assess how the provisions regarding data controllers' responsibilities under Decree 13 align with international data protection standards, identifying its progress and challenges. The analysis uncovers both convergence and divergence points between the related provisions under Decree 13 and the GDPR, particularly in terms of clarity, scope, and enforcement mechanisms. A significant challenge identified is the ambiguity in Decree 13's provisions on data controllers' responsibilities and the absence of several essential elements, which could undermine the effectiveness of Vietnam's data protection framework. To address these issues, the article offers strategic recommendations for legislative improvements and practical adjustments for data controllers in Vietnam. In conclusion, while navigating the path to a comprehensive data protection framework poses challenges for Vietnam, this journey offers an opportunity to align with regional and global developments in data protection laws. By learning from the GDPR and adapting to its specific features, Vietnam can develop a robust, effective, and trustworthy data protection environment, safeguarding its citizens' privacy rights and facilitating a favorable international business climate.

Keywords: Data controllers, personal data protection, accountability principle, GDPR, Vietnam Personal Data Protection.

* Corresponding author.
E-mail address: anhdk@ftu.edu.vn

https://doi.org/10.25073/2588-1167/vnuls.4610

1. Introduction

In the digital age, safeguarding personal data emerges as a paramount concern, necessitating stringent oversight of data controllers' responsibilities. Globally, nations grapple with the complexities of data protection, with Europe leading the way through its comprehensive General Data Protection Regulation (GDPR). This regulation has set a precedent, defining the responsibilities and expectations placed upon data controllers in an era where data breaches and privacy violations frequently make headlines, highlighting potential threats to individual rights and national economies.

Parallel to Europe's strides, Vietnam, with its burgeoning digital economy, has recently made significant advancements in data protection. This is evidenced by the recent enactment of Decree No. 13/2023/ND-CP on Personal Data Protection (Personal Data Protection Decree - Decree 13). In a practical respect, it is essential to acknowledge that Vietnam has historically grappled with challenges related to the unauthorized trading of personal data [1]. This issue commonly involves service providers responsible for managing customer data and granting access to unauthorized third parties. These third parties often engage in the subsequent transfer and trade of this data [2]. This situation underscores the ongoing necessity for more comprehensive legal regulations in this area. Vietnam's development of Decree 13 indicates a growing recognition of the vital role of data protection rules in this technologically advanced age [3].

This article delves into an in-depth analysis of the responsibilities of data controllers under the GDPR, comparing these with Vietnam's regulations. We begin by unpacking the definitions of personal data and data controllers, addressing the practical approach to attain controllership status. This is followed by a comprehensive examination of their responsibilities under both the GDPR and Decree 13, exploring data controllers' specific duties and expectations as regulated under both legal frameworks.

This comparative analysis aims to illuminate the parallels and divergences between the GDPR and Decree 13. It will not only highlight the challenges Vietnam may encounter in its journey towards robust data protection but also provide pragmatic suggestions for enhancing its approach. Understanding these frameworks in general and the responsibilities of businesses as data controllers in particular is not just an academic exercise but a vital perspective in helping Vietnam develop an effective data protection framework.

2. The Concepts of Personal Data and Data Controllers

2.1. The Concept of Personal Data

The concept of “personal data” is pivotal in shaping the scope and application of the regulation, emphasizing the objective of protecting individual privacy in the digital era. According to Article 4(1), personal data can be defined as any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [4].

Additionally, Recital 14 sentence 2 mentions information on legal persons can also fall within the scope of personal [4]. For example, data from a legal entity, such as a company name or email, that can be linked to an individual-often seen in small or family-owned businesses-is considered personal data [5].

The GDPR thus defines “personal data" in broad terms, aligning with its primary goal to protect the privacy and related interests of individuals in the informational realm.

Decree 13 also offers a broad definition of personal data, though its scope is slightly narrower. Article 2.1 of the Decree describes personal data as "any information expressed in forms such as symbols, text, digits, images, sound, or similar forms in an electronic environment, associated with or identifying a specific natural person". Like the GDPR, Decree 13's definition encompasses a wide array of information that relates to a person and that which can identify a person.[1] However, it is more limited than the GDPR in two ways: it specifies the forms of information (symbols, text, digits, images, sound, or similar forms in an electronic environment) and clarifies that personal data pertains only to natural persons, excluding data related to legal persons.

In conclusion, the nuanced definitions of "personal data" within the GDPR and Decree 13 reflect a fundamental commitment to individual privacy rights in the digital age. Yet, they also illustrate distinct approaches in the breadth of their coverage and the specific types of data they encompass.

2.2. The Concept of Data Controllers

The concept of a data controller is fundamental in data protection law, as it identifies who is primarily responsible for complying with data protection rules and ensuring the rights of data subjects. Article 4(7) of the GDPR defines a data controller as "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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" [4]. This provision outlines five key elements constituting the concept of a data controller: i) "the natural or legal person, public authority, agency or other body"; ii) "determines"; iii) "the purposes and means"; iv) "alone or jointly with others"; v) "of the processing of personal data".

Given the controller's role in ensuring accountability and protection of personal data, the Court of Justice of the European Union has emphasized that this concept should be broadly interpreted [6]. These five elements are all taken into account to define whether a business achieves controllership status or not. However, given the functional character of this concept, the determining factor that labels a data controller on a commercial legal entity is the actual roles the entities play and the actual influence. This indicates that being recognized as a controller is primarily based on its practical operations, not just on the formal designation of an actor as being a controller, such as in a contract [7].

A classic example of attaining controllership status through factual control is the SWIFT Case [8]. In this case, the idea that "an entity may be deemed a controller even if it exceeds its formal legal mandate" highlights the practical interpretation of the term "controller" in data protection law. When applied to SWIFT, this concept means that even if SWIFT's official responsibilities or mandates did not explicitly encompass certain data processing activities, if they factually undertook those activities (like transferring data to U.S. authorities), they could still be considered as a "controller" for those actions in the eyes of the law. Even though their cooperation with U.S. surveillance might not have been a part of their formal, contractual obligations with individual banks or customers, their factual role in transferring data meant they were potentially still accountable as a controller under EU data protection law.

This approach is particularly suited to the contemporary digital ecosystems, where businesses engage with their users through digital accounts. For example, many social media platforms process user preferences to

[1] Under Article 2(2), personally identifiable information is defined as "any information that is formed from the activities of an individual and, when used with other maintained data and information, can identify such particular natural person".

tailor their advertisement recommendation algorithm. Similarly, in the banking sector, the processing of personal data encompasses an array of activities: from collection, recording, and analysis to confirmation, storage, and modification. Both examples highlight the involvement of personal data and significant influence over such data, classifying these entities as data controllers.

The definition of a data controller under Decree 13 largely mirrors this approach, albeit with minor differences. Article 2.9 of the Decree defines a personal data controller as "an organization or individual that decides on the purpose and means of personal data processing". Like the GDPR, Decree 13 emphasizes actual control by regulating who "decides" and focuses on the "purpose and means of the personal data processing". Unlike the GDPR, Decree 13 is silent on whether a data controller can decide the purpose and means of data processing *alone or jointly with other parties*. Consequently, the concept of "joint controllers" under the GDPR is not present in Decree 13. This omission results in much ambiguity over the responsibilities of an organization that partially or jointly controls data with others.

In conclusion, despite minor differences, under both Decree 13 and the GDPR, the determination of a controller's status relies not just on legal authority but on actual control over data processing. This perspective highlights the real-world activities and influence a business has over personal data, aligning with the principle that accountability for data protection should reflect the reality of decision-making and influence in data processing, even when these decisions extend beyond formal agreements or statutory mandates.

3. Responsibilities of Data Controllers Under the GDPR

The GDPR establishes a robust mechanism to impose responsibilities on data controllers, reflected in two key aspects. The first, outlined in Article 5(2), is the principle of accountability. This principle primarily requires controllers to be responsible for and demonstrate their compliance with data protection regulations. The second aspect encompasses the specific responsibilities of data controllers in ensuring data protection, as stipulated under Articles 24 and 25 of the GDPR. Each of these aspects will be analyzed in detail.

3.1. Principle of Accountability

The issue of data violations has become increasingly alarming due to technological advancements. A report issued in 2020 estimated that 64.2 zettabytes of data were generated, captured, and used worldwide [9]. The sheer volume of data processed daily presents not only heightened threats but also an urgency to take necessary actions to safeguard data subjects. More importantly, the increasing flow of individuals' information globally is closely connected with its rising economic value and other relevant benefits. One way personal information being monetized is by giving advertising companies access to users' preferences collected via online platforms. For example, top social media channels, such as LinkedIn Marketing Solutions, earned $3 billion in ad revenue in 2020 [10], demonstrating the value of personal information and its vulnerability to exploitation.

Given the longstanding existence of data protection mechanisms in some legal systems, the question arises as to what viable solutions exist for these threats. Traditionally, these mechanisms have not obligated data controllers to actively engage in data protection programs. Thus, the principle of accountability has emerged as a foundational approach to addressing these challenges.

This principle aims to ensure that all bodies governing data processing take a proactive role in protecting individuals' information and demonstrate their actions. While this principle is recognized in other national and international instruments, the EU only recently incorporated it

into its regulations. The only implicit indication of this principle is stated in Article 6(2) of the Data Protection Directive (also called Directive 95/46/EC or DPD): "It shall be for the controller to ensure that paragraph 1 is complied with". Notably, this implication was insufficient to steer controllers towards stringent data protection schemes. However, the principle of accountability fundamentally reshapes data protection regulations in the EU and lays the foundation for more rigorous and comprehensive protection against data breaches and violations.

Article 5(2) of the GDPR states, "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')". This article, found in Chapter 2, "Principles", indicates that accountability is one of the seven fundamental core principles of the Regulation. This significant change marks considerable progress in EU legislation compared to Directive 95/46/EC. Specifically, accountability in the GDPR includes two major factors: "responsible for" and "able to demonstrate compliance." The latter acts as a complementary element to the former, activating a two-layer responsibility mechanism to prevent misconduct.

In summary, accountability in this context can be defined as "proactive and demonstrable organizational responsibility" [11]. However, this definition does not fully capture the extensive scope of this principle as stated in the GDPR. As further examined, accountability should be considered a term with a unique meaning.

3.2. Specific Responsibilities

Provisions in Article 24 and Article 25, Chapter 4, "Controller and Processor" of the GDPR, clearly demonstrate the accountability principle mentioned in Article 5(2). While Article 24 focuses on the general interpretation of the accountability principle, Article 25 reinforces the obligations of controllers in a proactive and effective manner.

Under these articles, data controllers must fulfil two main sets of responsibilities: first, the responsibility to implement appropriate technical and organizational measures (TOMs), and second, the responsibility to demonstrate compliance under the GDPR. These requirements are analyzed both statutorily and practically.

3.2.1. Responsibility to Implement Appropriate Technical and Organizational Measures

The first specific responsibility of data controllers under the GDPR is to implement appropriate technical and organizational measures. A primary question arises regarding what types of measures are deemed appropriate under the GDPR. Unfortunately, Articles 24 and 25 do not provide a clear and explicit answer. This lack of specificity has led to concerns about the regulation's flexibility and potential uncertainty, posing challenges for both controllers and supervisory authorities in evaluating the appropriateness of these measures. However, this vagueness is designed for specific reasons.

Firstly, pursuant to Article 24(1), data processing varies significantly in terms of "nature, scope, context, and purposes" [4]. "Nature" refers to the methods used by controllers to process data. "Scope" indicates the amount of data processed, its sensitivity, and the extent of its impact on data subjects [12]. "Context" involves the circumstances of data processing, such as the number of involved parties and the modernity of techniques. "Purpose" signifies the ways of using the processed data. The diversity of these factors results in numerous scenarios, making standardization impractical in the Regulation.

Secondly, Article 24(1) introduces the principle of proportionality regarding the risks to the "rights and freedoms of natural persons". This principle suggests that higher risks require more stringent measures. Entities dealing with high-risk data such as credit card numbers, passports, and health records should implement stricter regulations. Conversely, those processing lower-risk information may adopt

less stringent measures. The size of an organization is not always proportional to the intensity of the measures, as smaller entities may still process high-risk data. To complement article 24(1), recital 75 establishes an extensive list of possible risks that may "lead to physical, material or non-material damage". According to this list, there are six major groups of risks, including damages to personal identity (discrimination, reputation, identity theft), damages to economic and social status, disclosure of sensitive data (religion, political opinion, ethnicity, location), deprivation of self-control over personal data, children-related and mass processing (a significant amount of data and data subjects included) [4].

Thirdly, controllers should pay attention to the terms "the state of the art" and "the cost of implementation" in Article 25. "The state of the art" requires organizations to consider the development status of the technologies implemented. This encourages controllers to revise and renew the measures and discourages obsolescence constantly. In other words, controllers must be aware of the "current progress in technology that is available on the market... and technological advances" [13]. Meanwhile, "the cost of implementation" is to prevent any unreasonable excuses due to high costs or over budget. The controllers are given broad discretion to choose measures that are in line with their financial capacity.

For the three mentioned reasons, the lack of specifications under Article 24 and Article 25 is designed to allow sufficient flexibility in practice. It requires the determination of appropriate measures on a case-by-case basis, taking into account two factors outlined in Article 24(1) and one factor in Article 25(1).

The second issue is the definition of TOMs since GDPR does not provide the meaning of "technical and organizational". Some scholars have put forward some worth considering proposals. For example, the technical factor is anything related to technological means ("devices, network, hardware") [14], which tends to be restricted within the mechanical scope. Meanwhile, "organizational" refers to actions affecting the structure or the person inside an organization, which is generally more flexible and diverse. From the viewpoint of the author, an analogy can be drawn between the terms "technical and organizational" and the hardware and software of a computer. The hardware part of the computer allows it to function properly, yet it is essentially useless unless accompanied by the software. Similarly, technical measures play a fundamental role in the data protection system. Without such underlying measures, data processing is prone to be compromised and stolen for malicious purposes. Meanwhile, organizational measures act as the glue that binds all measures together, strengthening the overall protection structure.

While the lack of definition is well-founded, it is still troublesome to visualize these measures in practice. Consequently, in its Opinion, the Article 29 Working Party (WP29) issued a non-exhaustive and referential list of common measures [15]. It suggested ten measures, which can be summarized and categorized as follows: preparatory, in-progress, problem-solving and assurance measures. During the preparatory phase, controllers are expected to introduce a series of internal policies (data compliance, security principle, notice) [15] and procedures (self-assessment, preview) to control the processing operations. Besides, they should organize mandatory training for employees and managers who are involved in data processing. The in-progress stage requires the appointment of a professional, such as external DPOs or internal supervisors, to oversee the actual process to ensure compliance mapping processing activities to assess purposes and possible risks [11]. Problem-solving measures, which are designed for repairing any unwanted breaches, consist of a "complaints handling mechanism" [15]; notification of breaches or deficiencies, and conduct of "privacy impact assessment" when necessary. Lastly, assurance includes verification of implementing these measures in reality via audits, independent

certification and transparency "for data subjects, regulators, and the general public" [11].

Among the suggested measures, the implementation of data protection policies is re-emphasized pursuant to Article 24(2). In this provision, the principle of proportionality acts as the deciding factor of the conditions under which such policies are compulsory. Organizations that conduct sophisticated and sensitive data processing operations are legally required to introduce larger numbers of binding policies than those that handle simple and lower-risk personal information.

In addition, Article 25 takes a step further by requesting controllers to implement TOMs to fulfil the principle of privacy by design and by default. Upon initial observation, by design and by default, they are similar; all aim at safeguarding individual's information and legitimate rights. However, by design, it covers a broader scope of measures, focusing on the whole data processing, especially the outset. Its goal is to ensure a "proactive not reactive; preventative not remedial" [16] approach by controllers. An example of achieving the "by design" requirement is pseudonymization. Pursuant to Article 4(5), processed personal information should not be traceable to an "identified or identifiable natural person" [4] without the additional information, which shall be stored separately. For example, a student's full name or phone number after processing exists under the form of an abbreviation or "XXX", and this person is only identified through a separate source of information such as his or her major at school. It is also significant for controllers to distinguish pseudonymization and anonymization as the former is a reversible process and remains a connection with the data subject, while the latter permanently removes the link and is no longer considered personal data protected under GDPR. On the other hand, by default, directs the attention to the outcome of the process, guaranteeing that personal data is automatically protected ("built into the system") [16] and "are not made accessible without the individual's intervention" in accordance with Article 25(2) [4]. This concept is fulfilled in view of four fundamental principles mentioned in Article 5(1) GDPR, including data minimization, purpose specification, storage limitation and confidentiality [4].

Besides, controllers must review and update the implemented TOMs when necessary. The term "necessary" was a major change compared to the GDPR draft, providing the proposed time was two years [11]. To begin with, regular reviews and updates are to evaluate the effectiveness of the implemented measures since they are not always appropriate and effective. Therefore, a fixed timeline for renovation appears to be rigid and untimely. Instead, the term "necessary" offers a more flexible approach, allowing controllers to take actions regardless of frequency or intensity as long as this requirement is necessary. This provision also enshrines the spirit of accountability principle, which grants controllers a proactive role in their protection schemes. The controllers must act independently and actively to ensure their operations are in accordance with the Regulation.

3.2.2. Responsibilities to Demonstrate Compliance

The second specific responsibility of data controllers under the GDPR is to demonstrate compliance. This is a new obligation compared to Directive 95/45/EC. It requires controllers to provide evidence of their compliance with the GDPR to external entities, including supervisory authorities, data subjects, and the general public. In practice, the extent of this duty aligns with the principle of proportionality, meaning the classification and depth of proof should correspond to the level of risks involved in data processing. Higher risks necessitate more thorough proofs.

Article 24(3) of the GDPR outlines two primary methods for demonstrating compliance: approved codes of conduct (COD) and certification mechanisms. Another way is through guidance by the Board and indications provided by a data protection officer, as stipulated in recital 77 [4].

Article 40 of the GDPR governs the approval process for CODs. The main aim of a COD is to

facilitate the actual application of the Regulation [4], as tested against eleven elements listed in Article 40(2). A COD must undergo a rigorous process of drafting, amending, or extending to receive authorization. The requirements intensify for CODs overseeing cross-border processing within EU Member States, as they must receive an official opinion from the EU Data Protection Board and a final decision from the Commission. Post-implementation, CODs are monitored according to Article 41, ensuring compliance without encroaching on the supervisory authorities' tasks and powers [4].

Certification mechanisms, such as certifications, seals, and marks, also demand extensive proof of compliance, subject to approval by the Board or other authorities. Notably, Article 42(7) only extends the certification validity to three years maximum [4] and can be revoked if there are signs of misconduct or unmet approval conditions. Holding a certification does not reduce the controllers' obligation to comply with the Regulation. Article 24(3) clarifies that these mechanisms "may be used as an element" of compliance, indicating that they are partial indicators and not conclusive proof of compliance. Therefore, controllers are tasked with concurrently implementing measures and demonstrating compliance.

4. Responsibilities of Controllers under Vietnam's Personal Data Protection Decree

On July 1st, 2023, Vietnam enacted the Personal Data Protection Decree (Decree No. 13/2023/ND-CP - hereinafter referred to as "Decree 13"), representing a pivotal development in the nation's data protection framework. This Decree, which evolved through extensive public consultation and amendments over five months, is celebrated as a landmark in establishing a data protection regime in Vietnam where none previously existed. Its notable features include an expanded definition of data, applicability to both domestic and international entities, a detailed enumeration of sensitive personal data, and specific protections for minors. Despite its recent implementation, Decree 13 is anticipated to significantly contribute to creating a legally harmonious environment. This concentrates on elucidating the responsibilities of controllers as stipulated in Decree 13.

Article 38 of Decree 13 delineates seven key responsibilities for data controllers. These responsibilities encompass i) implementing TOMs to demonstrate compliance, review and update when necessary; ii) mapping data processing operations; iii) notifying data breaches to competent bodies; iv) selecting qualified data processors; v) protecting data subjects' legitimate rights; vi) taking responsibilities in the event of damages; vii) cooperating with state agencies [17]. Unlike the GDPR, which disperses responsibilities across various sections, Decree 13 consolidates these duties into a singular article, facilitating a more straightforward identification of obligations for controllers. This collective method is beneficial in terms of assisting controllers in quickly identifying their responsibilities.

In examining the nuances of Vietnamese laws on data protection, several aspects warrant attention. Firstly, Article 38 emphasizes the necessity for controllers to implement TOMs and to review and update these measures regularly. A notable inclusion is the directive to record or map data processing operations daily, an element absent in the GDPR. This requirement not only ensures law-abiding processing but also serves as substantial evidence of compliance in case of data breaches. It further aids in identifying potential violations, enabling controllers to promptly undertake preventive actions and secure the overall data processing system. Thus, Article 38(2) encapsulates the ethos of a "preventative, not remedial" approach to data protection.

Furthermore, Article 38 of Decree 13 echoes the spirit of data protection law underscored within the GDPR. This congruence with international legal frameworks, especially the

GDPR, is evident in key mandates like the obligation to implement TOMs, demonstrate compliance with data protection norms, and continuously revise these measures in response to emerging threats and best practices. This alignment with global standards underscores the notion that data controllers worldwide ought to adhere to certain fundamental principles, ensuring conformity with strict and universally accepted guidelines.

In addition, Decree 13 casts data controllers in a proactive role. Controllers are tasked not only with protecting data subjects' rights through organizational and technical measures but also with proactively reporting violations as stipulated in Article 23. The mandate for breach notification is particularly laudable. By making it obligatory for entities to report breaches, the decree diminishes the likelihood of cover-ups, fostering a climate of transparency and trust. Consequently, data subjects, reassured of being informed about any mismanagement of their data, are likely to be more willing to entrust their data to organizations. Accordingly, this fosters a collaborative approach between data controllers and subjects in devising timely corrective measures.

Despite the potential advancements presented by Article 38, its practical implementation poses significant challenges. For instance, Decree 13 does not explicitly include the "accountability principle", a key concept long recognized in national and international data protection laws, including the GDPR. Although Article 3(8) can be interpreted as a literal Vietnamese translation of GDPR's Article 5(2), encompassing the dual responsibilities to comply and demonstrate compliance, the absence of an expressly acknowledged term dilutes the emphasis on this core principle in data protection law. Moreover, this omission not only undermines the gravity of controllers' tasks but also signifies a critical divergence between the Vietnamese legal system and global standards, potentially confusing international entities operating in Vietnam. The non-recognition of "accountability" in Vietnamese law, beyond Decree 13, lowers the awareness among legislators, government bodies, and legal entities about their collective role in safeguarding individual information.

In addition, Article 38(1) of Decree 13 encapsulates the essence of GDPR's Article 24(1) by mandating controllers to implement TOMs and "safety and security" measures to "demonstrate that data processing aligns with the law". While this seems identical to GDPR provisions at first glance, Decree 13 omits the explicit responsibility to comply with data protection law, focusing instead on the need for controllers to "prove" compliance. This discrepancy raises questions about the efficacy of TOMs and safety measures in demonstrating compliance under Decree 13 and whether the act of demonstrating compliance supersedes actual compliance. Furthermore, the absence of a defined protocol for evidence of compliance in Vietnamese law compared to the EU's code of conduct or certification requirements jeopardizes controllers' ability to validate their legal adherence, potentially discouraging commitment to data protection and exposing them to violations. This conflict may also encourage passive and deceptive practices aimed at superficial compliance rather than genuine adherence, a concern since actual compliance is fundamental.

Moreover, the lack of guiding instruments regarding TOMs and "safety and security" measures under Decree 13 leaves a considerable gap for controllers in selecting appropriate measures. This ambiguity poses concerns about how supervisory authorities will assess the effectiveness of these measures in practice, diminishing the directive's controlling power due to its indistinctness and uncertainty. This issue is further compounded in Article 38(4), which allows controllers to cooperate only with qualified processors who align with the processing objectives and have implemented suitable protection measures. This provision, while aimed at ensuring alignment with

processing goals, inadvertently limits controllers' choices and complicates the evaluation of processors' suitability.

Finally, Decree 13 does not establish a comprehensive sanctioning mechanism. Although Article 38(6) notably specifies controllers' liability for damages caused by data processing, this liability is not translated into concrete sanctions. In contrast, the GDPR explicitly outlines monetary penalties for non-compliance, thus motivating controllers to adhere to regulations to avoid severe financial repercussions. The absence of specific sanctions in Decree 13 may lead to a nonchalant attitude among controllers regarding the consequences of their actions, undermining the commitment to a lawful environment.

In short, while Decree 13 marks a significant step forward in Vietnam's data protection landscape, it encounters challenges in implementation and alignment with international standards. Addressing these issues will be pivotal for Vietnam to fortify an effective and robust data protection regime.

5. Strategic Recommendations and Concluding Insights

The comparative analysis of the European Union's General Data Protection Regulation (GDPR) and Vietnam's Personal Data Protection Decree (Decree No. 13/2023/ND-CP) sheds light on vital areas for improvement within Vietnam's developing data protection framework. Decree 13, while being a significant step, is marked by notable challenges, including its lack of clarity and the omission of key foundational elements. This section offers a set of integrated recommendations aimed at both the Vietnamese government and the business sector, culminating in a discussion on the wider implications for the evolution of data protection in Vietnam. Given that a decree functions as a regulatory instrument issued by the executive branch, which is subordinate to formal legislation, there is an anticipation for the eventual enactment of a comprehensive Data Protection Law in Vietnam [18]. The recommendations provided herein are intended to inform and support the ongoing advancement of personal data protection in the country.

For the legislation, it is paramount to refine the Personal Data Protection Decree to align more closely with international data protection standards, as exemplified by the GDPR. This entails introducing precise terminology to clarify the responsibilities of data controllers, particularly in defining the conditions for evaluating the appropriateness of technical and organizational measures (TOMs). Drawing from the GDPR's approach, which considers factors like nature, scope, context, and technological advancement, Vietnam could tailor these criteria to its unique socio-economic context. This could involve issuing supplementary instructions that provide detailed guidance on implementing TOMs and safety measures, considering the country's current technological and economic landscape.

Moreover, there is a need for a more robust punitive framework for violations of the data protection regulations. The introduction of stringent penalties, including substantial administrative fines and potential criminal charges, would serve as a deterrent against non-compliance [3]. This shift should be accompanied by a principle of proportionality, ensuring that fines are commensurate with the severity of the infringement and the financial capacity of the data controller. Further, instituting mandatory compensation for data subjects whose rights are infringed upon would reinforce a culture of accountability.

For data controllers in Vietnam, they should proactively adapt their practices to comply with the evolving data protection regime. This includes public commitments to data protection, enhancing transparency about data usage, and investing in technological upgrades to meet international standards. Establishing internal data management departments staffed with trained professionals could further entrench a culture of compliance and proactive risk management within organizations.

In conclusion, though at a nascent stage, data protection in Vietnam is poised for significant evolution. The GDPR's comprehensive and rigorous approach offers a valuable blueprint for Vietnam to enhance its legal framework. As the country continues to grow digitally and expand its e-commerce footprint, aligning with international data protection standards is not just advantageous but essential. Such alignment ensures the safeguarding of individual privacy rights while facilitating Vietnam's participation in the global digital economy.

The journey towards establishing a comprehensive data protection framework in Vietnam is undoubtedly challenging; however, it offers an opportunity for the nation to position itself within the evolving landscape of global data protection. By learning from the GDPR and adapting to the specific needs and nuances of its own digital ecosystem, Vietnam can create a robust, effective, and trustworthy data protection environment. This journey is crucial not only for safeguarding the privacy rights of its citizens but also for fostering a favorable international business environment.

References

[1] H. Chu, Legal Framework for Personal Data Protection in Vietnam, in T. Phan and D. Damian (eds.), Smart Cities in Asia, SpringerBriefs in Geography, pp. 91-96, https://doi.org/10.1007/978-981-19-1701-1 (accessed on: September 25th, 2023).

[2] T. T. T. Phuong, The Laws on the Protection of Personal Information in some Countries and Recommendations for Vietnam, Hanoi Law Review No. 8, 2020, pp. 42.

[3] J. M. Scheil, New Data Protection Regime in Vietnam, Overview of Emerging Parallels to GDPR, Computer Law Review International 3/2023, pp. 73-77.

[4] EU General Data Protection Regulation (GDPR): 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed on: September 25th, 2023)

[5] C. Kuner, Lee A Bygrave, Christopher Docksey, The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, London, 2020, pp. 111

[6] Case C-131/12, Google Spain SL v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014 (Grand Chamber) (ECLI:EU:C:2014:317), paragraph 34, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131; Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, judgment of 5 June 2018 (Grand Chamber) (ECLI:EU:C:2018:388), paragraph 28, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210); Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW e.V., judgment of 29 July 2019 (ECLI:EU:C:2019:629), Paragraphs 65-66, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62017CJ0040 (accessed on: September 25th, 2023).

[7] Case C-25/17, Jehovan Todistajat, Paragraph 21 (Noting that in Particular, the "Effective Control" Must be Taken into Account), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62017CJ0025; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62017CC0025 (accessed on: September 28th, 2023).

[8] Article 29 Working Party (3), Press Release on the SWIFT Case Following the Adoption Of Article 29 Working Party Opinion on The Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 06/EN, pp. 3.

[9] P. Taylor, "Amount of Data Created, Consumed, and Stored 2010-2020, with forecasts to 2025", Statista, https://www.statista.com/statistics/871513/worldwide-data-created/, 2023 (accessed on: September 25th, 2023).

[10] M. Graham, Microsoft Says Linkedin Topped $3 Billion in ad Revenue in the Last Year, Outpacing Snap and Pinterest, April 2021, https://www.cnbc.com/2021/04/27/microsoft-linkedin-topped-3-billion-in-ad-revenue-in-last-year.html (accessed on: September 25th, 2023).

[11] C. Kuner, Lee A Bygrave, Christopher Docksey., The EU General Data Protection Regulation

(GDPR): A Commentary, Oxford University Press, London, 2020, pp. 561- 567.

[12] Jürgen Kühling/Benedikt Buchner, General Data Protection Regulation, Federal Data Protection Act: DS-GVO/BDSG, 3rd edition, C. H. Beck, 2020, Article 24, Margin Number 14.

[13] European Data Protection Board, Guidelines 4/2019 on Data Protection by Design and by Default, Version 2.0, 2020, pp. 8.

[14] E. Dravalou, What "Technical and Organisational Measures" Actually Means, Privacy Management Blog, 2021, https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/, (accessed on: September 25th, 2023).

[15] Article 29 Working Party (2), Opinion 3/2010 on the Principle of Accountability, 13/7/2010, 00062/10/EN, WP 173, pp. 11-12.

[16] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices", pp. 2.

[17] Decree, No. 13/2023/ND-CP on Personal Data Protection, https://luatvietnam.vn/dan-su/nghi-dinh-13-2023-nd-cp-bao-ve-du-lieu-ca-nhan-249791-d1.html (accessed on: September 25th, 2023).

[18] J. M. Scheil, New Data Protection Regime in Vietnam, Overview of Emerging Parallels to GDPR, Computer Law Review International 3/2023, pp. 73; V. T. Thuy, Several Issues on the Draft Decree on Personal Data Protection, Hanoi Law Review, No. 7 (266) 2022, pp. 88-90.