sciendo
Vietnamese Journal of Legal Sciences, Vol. 11, No. 02, 2024, pp. 01-13 DOI: 10.2478/vjls-2024-0007

THE REGULATION OF DATA TRANSMISSION IN THE DIGITAL ERA: FROM THE EUROPEAN UNION'S PERSPECTIVE AND IMPLICATIONS FOR VIETNAM

HOANG LE NGOC TIEN DAT
Faculty of Law, University of Debrecen, Hungary
Email: hoanglengoctiendat@gmail.com
CHU THI THANH AN
Géza Marton Doctoral School of Legal Studies, University of Debrecen, Hungary
Email: anthanhchu11@gmail.com

Abstract

Data transmission is crucial in the digital age, making robust legal frameworks for data protection and the free flow of information essential. Distinguishing between personal and non-personal data is critical for ensuring regulatory compliance. Roles like controllers and processors define obligations and remedies, ensuring secure and lawful data handling. Based on the analysis of the European Union perspective on the aforementioned aspects, the paper provides implications for Vietnam in addressing the regulatory gaps regarding data-related laws in general and data transmission in particular.

Keywords: *personal data, non-personal data, data transmission, EU, Vietnam*
Received: 13 May 2024 / Revised: 13 June 2024 / Accepted: 5 August 2024

In the modern era, data is crucial for advanced technologies like AI and machine learning. Regulating data transmission, processing, and management has been essential. The 2018 implementation of the General Data Protection Regulation (GDPR) in the European Union (EU)[1] has significantly impacted technical applications involving data and information activities.

GDPR employs several terms to refer to the movement of data from one location to another, namely the free movement of data, data flows, and data transfers.[2] Each of these terminologies has a distinct meaning within the context of GDPR. Free movement of data pertains to the processing of data across the borders of EU member states, because it could be connected to the four freedoms of the EU common market.[3] Data flows, on the other hand, encompass the travel of data across EU member state borders, as well as the transfer of data from the EU to third countries[4] so that it can be understood as any cross-border journey of data.[5] The term "data transfers" as defined in the Article 44 GDPR has a broad scope, referring to "any transfer of personal data

1 Regulation (EU) 2016/679 on the protection of natural person regarding the processing of personal date and on the free movement of such data.
2 Tobias, N. (2023), 'The restrictive effect of the legal mechanism for data transfers in the European Union', in: Tobias, N. (2023), 'Data protection without data protectionism', *European Yearbook of International Law*, Vol. 28, p. 135.
3 *Ibid*., p. 136.
4 Recital 101 of the GDPR.
5 Tobias, N. (2023), *supra* note 2, p. 137.

which are undergoing processing or are intended for processing after transfer to a third country or to an international organization".[6] In the context of GDPR, "data transfer" in Chapter V refers to making data available to third countries or international organizations, requiring that (i) the exporter is subject to GDPR, (ii) personal data is provided to another entity (importer), and (iii) the importer is in a third country or is an international organization, regardless of their GDPR liability per Article 3.[7]

From this notion, it can be inferred that data transmission is a practical form of data transfer as involving controllers and processors to enable data flow amongst parties.[8] Data transmission is the process of sending and receiving digital or analog data between the devices of parties.[9] Data transmission occurs through cables, optical fibers, or wireless methods and involves at least two digital devices interacting over a network. Key components are: (i) the sender, which initiates transmission, (ii) the receiver, which gets the data, (iii) the data or messages, including text, images, audio, video, and photos, and (iv) regulations on protected factors and free flow rules. Thus, data transmission is a subset of data transfer, focusing on sending data over a communication medium.

Data transmission, like other data-related activities, concerns the role of the data controller and data processor to uphold data protection principles and facilitate free data flow.[10] In the EU, data transmission must adhere to the GDPR principles, including transparency and proportionality, ensuring only relevant personal data is collected and processed, with clear communication to individuals about their data use.[11]

As Vietnam's data market grows and the country aims for a digitally transformed economy, its current legal framework on data transmission should adopt personal data protection principles.[12] In early 2024, the government approved the master plan for establishing a data market and piloting data transaction floors as key components of its national data strategy until 2030.[13]

6 *Ibid.*, p. 138.

7 European Data Protection Board (2023), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Version 2.0. Retrieved from: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en [accessed 9 June 2024].

8 Tobias, N. (2023), *supra* note 2, p. 138.

9 Margaret, R. (2023), 'What does data transmission means?'. Retrieved from: https://www.techopedia.com/definition/9756/data-transmission [accessed 30 April 2024].

10 Recital 6 and 82 of the GDPR.

11 Recital 4 and Article 5(c) of the GDPR.

12 Vietnam's data market had a value of 858 million USD in 2020, and it is projected to have a compound annual growth rate (CAGR) of 5.32% from 2023 to 2027. *See more at*: An Binh (2023), 'Thi truong du lieu cua Viet Nam mo ra nhieu co hoi' [Vietnam's data market opens up great opportunities]. Retrieved from: https://toquoc.vn/thi-truong-du-lieu-cua-viet-nam-mo-ra-nhieu-co-hoi-20230317103852314.htm [accessed 30 April 2024].

13 Decision No. 142/QD-TTg of 2 February 2024 approving the National Data Strategy by 2030.

Against the significant socio-technical development and expectations, the current legal framework on data transmission in Vietnam is inadequate in terms of three key issues: (i) identification of personal data and non-personal data as the prioritized stage requirement in data transmission; (ii) regulation on the obligations of controllers and processors to safeguard data protection and ensure the free flow of data; and (iii) remedies for data transmission violations.

The aim of this paper is to examine how the EU regulates data transmission to achieve data protection and remove impediments to the free flow of data, thereby drawing implications for Vietnam to improve its legal framework in this area. In section 1, the paper illustrates the importance of the identification of personal data and non-personal data as the prioritized stage for data transmission, followed by the analysis of key actors involved in this process, and remedies for violations of data transmission regulation. The empirical practice in Vietnam in terms of data activity detects and analyzes the regulation gaps is provided in section 2. The final section is reserved for the implications from the EU's perspective regarding the analysis and recommends several factors to tackle the present challenges in Vietnam in terms of data transmission.

1. The European Union regulation of data transmission

1.1. The identification of personal data and non-personal data

The acceleration of technology in the economy has led to diverse data types across all sectors. In the EU, the Data Retention Directive (2006/24/EC) previously listed data categories for retention, including: data to trace and identify the source, destination, date, time, duration, means of communication, user's equipment, and location of mobile communication equipment.[14] These data enabled identifying the contact details, time, and location of communications, as well as the frequency of conversations between a subscriber and specific individuals.[15] Therefore, recognizing personal data protection as a fundamental human right[16] has highlighted the need to distinguish between different data categories,[17] leading to the clear classification of data into personal and non-personal data.[18]

According to GDPR, personal data contains data pertaining to natural person as long as they can be identified, either directly or indirectly, is said to be identifiable.[19] Article 8 of the EU Charter of Fundamental Rights

14 Article 5 of the Data Retention Directive (2006/24/EC).

15 *Joined Cases C-293/12 and C-594/12*, EU Court of Justice (8 April 2014), para. 26.

16 Article 8 and Article 16 of the EU Charter of Fundamental Rights.

17 Recital 5 of the Directive 2002/58/EC.

18 Recital 7 of the Regulation 2023/2024.

19 Article 4(1) of the GDPR. *See more at*: Raphaël, D. (2020), 'Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?', *Regulation & Governance*, Vol. 16, No. 1, pp. 156-176.

enshrines the principle that personal data cannot be transferred without explicit consent from the data subject. It establishes a two-fold mechanism: (i) personal information must be handled fairly, used only for intended purposes with the subject's consent or another legal basis, and (ii) individuals have the right to access and correct their personal data.

Alongside its protective regulations, GDPR also aims to facilitate the free flow of data.[20] GDPR lays down the principles of fair, transparency, and proportionality to unseal the flow of data as long as controllers and processors can operate technical and organizational measures for non-personal data.[21] Non-personal data is any information that is unrelated to a specific or identifiable living person, otherwise it is information that was formerly private but was subsequently turned anonymous and cannot be connected to a specific individual.[22] In principle, data protection rules should not apply to data that is not related to an identified or identifiable natural person, or to personal data that has been made anonymous in a way that makes the data subject unidentifiable.[23] Thus, non-personal data is specifically categorized for aspects such as data governance,[24] open data,[25] and harmonized rules on fair access to and use of data.[26] Regulation 2018/1807 on the free movement of data specifies examples of non-personal data, including precision farming data for optimizing pesticide and water use, aggregated and anonymized datasets for big data analytics, and industrial machinery maintenance requirements data.

In addition, the intersection point between the above two categories is classified as pseudonymous data. According to GDPR Recital 26, pseudonymous data includes "additional information" that could potentially link it to specific data subjects, unlike anonymous or non-personal data, making it crucial to assess the presence of such information to distinguish between anonymous and pseudonymous data.[27] Despite not requiring

20 Recital 3 of the GDPR.

21 Recitals 4, 39, and 58 of the GDPR.

22 YourEurope, 'Free flow of non-personal data'. Retrieved from: https://europa.eu/youreurope/business/running-business/developing-business/free-flow-non-personal-data/index_en.htm#:~:text=Non%2Dpersonal%20datasets%20refer%20to,way%20to%20a%20specific%20person, [accessed 30 April 2024].

23 Recital 26 of the GDPR.

24 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

25 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). See more: Tim, H. (2020), 'Sharing is caring – Data sharing initiatives in healthcare', *International Journal of Environmental Research and Public Health*, Vol. 17, No. 9, p. 3046.

26 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

27 *Case T-557/20*, EU Court of Justice (26 April 2023), para. 81.

additional identification information, pseudonymized data is still subject to GDPR under Article 11. Article 5.1(f) emphasizes pseudonymization as a risk management measure, showcasing the controller's commitment to data security. Recital 29 supports pseudonymization within the same controller with proper safeguards, promoting its use for data protection. However, pseudonymized data can still be linked to individuals via online identifiers like IP addresses or cookie IDs, as highlighted in Recital 30. Even a search engine is an element to identify liability[28] when data published or placed on the internet by third parties is found by a search engine.[29] When data is transmitted in the internet as a means of transferring it to a host provider,[30] the controller is liable for any harm that may occur to the data subject without their consent.

Distinguishing between personal data and non-personal data is a critical step in determining the regulatory framework that applies to data transmission, particularly given the rising volumes of generated and exchanged data.[31] The challenge lies in profiling personal data, where the increasing speed of data generation complicates maintaining anonymity and protecting personal information.[32] In any case, data controllers and processors as the key actors to monitor and swiftly implement organizational and technical safeguards.

1.2. Key actors involved in data transmission

The analysis emphasizes distinguishing between personal and non-personal data in transmission, noting the risk of linking non-personal data to personal data. EU law assigns key roles to data controllers and processors to implement safeguards and address these risks.

1.2.1. The concepts of data controller and processor

Article 4.7 of the GDPR defines a data controller as an individual, organization, public authority, or other body that, alone or jointly with others, determines how and why personal data is processed. This includes joint controllers who collectively decide on data processing methods and objectives, requiring clear delineation of roles for GDPR compliance.[33] Ultimately, the capability to decide the purposes and methods of processing personal data distinguishes the controller as the key entity responsible for identifying information about natural persons.[34]

28 *Case C-131/12*, EU Court of Justice (13 May 2014), para. 38.
29 *Ibid*., para .100(1).
30 *Case C-101/01*, EU Court of Justice (6 November 2003), para. 100(1).
31 Michèle, F., and Frank, P. (2020), 'They who must not be identified-distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law*, Vol. 10, No. 1, pp. 11–36.
32 Recital 9 of the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the EU.
33 Recital 26 of the GDPR.
34 *Ibid*.

GDPR provides several examples of purposes for processing data such as direct marketing,[35] archiving,[36] scientific research purposes,[37] statistical purposes.[38] Regardless of the means used to transmit, they are all regulated by the responsibility of being data controller, and their mutual is one goal that is to protect personal data by appropriate technical and organizational measures.[39] Under Regulation 2023/2854, a user is deemed a controller when operating as an enterprise, not as a data subject in shared household use. According to Article 6(1) of the GDPR, such users must justify accessing personal data from connected products or services, typically through consent or contractual obligation with the data subject. Joint controllers under Article 26 of the GDPR must clearly define their roles through mutual agreement to comply transparently.[40]

A data processor, whether an individual, organization, or government agency, manages personal data on behalf of the controller without assuming the role of data owner.[41] This responsibility includes carrying out specific tasks assigned by the controller to facilitate data availability, as stipulated in the requirement to "process personal data on the controller's behalf".[42] According to Article 4(2) of the GDPR, processing encompasses a wide array of activities from data collection to destruction. The processor must act strictly in the controller's interest,[43] adhering to instructions and employing suitable technical and organizational measures. Any processing must be governed by a binding agreement, allowing flexibility in choosing contractual clauses or creating custom agreements to ensure compliance with data protection regulations.[44]

1.2.2. Obligations of data controller and processor in data transmission

The roles of the data controller and processor are crucial in data transmission. Despite differing responsibilities for personal and non-personal data, both must implement necessary safeguards to comply with data protection laws. This duty covers both the design and actual processing of data.[45]

35 Recital 70 of the GDPR.
36 Recital 158 of the GDPR.
37 Recital 159 of the GDPR.
38 Recital 162 of the GDPR.
39 Article 24 of the GDPR.
40 Recital 34 of the Regulation 2023/2854.
41 Article 4.8 of the GDPR.
42 Recital 22 of the Regulation (EU) 2023/2854.
43 According to Article 28(10) of the GDPR, a processor violates the Regulation when it begins to choose its own goals and methods of processing instead than following the controller's instructions.
44 European Data Protection Board (2021), *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Version 2.1. Retrieved from: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf [accessed 30 April 2024].
45 Article 25 of the GDPR.

Regarding personal data, the GDPR governs the obligations of data controllers from the moment they collect data from individuals.[46] A notable aspect of the GDPR is the introduction of a set of meta-regulatory obligations on data controllers.[47] Key principles include accountability,[48] requiring controllers to not only comply with GDPR but also demonstrate compliance.[49] The law also imposes an obligation on either public or private entities to retain or provide certain data.[50] This involves defining lawful purposes for data collection, ensuring data accuracy, and implementing measures to maintain confidentiality and integrity. Transparency mandates controllers inform individuals clearly about data processing, detailing what data is collected, why, and how it's used (Article 12 to Article 14).[51] Technical and organizational measures are essential to mitigate risks in data processing, integrating data protection into operations from inception.[52] These measures ensure data security, limiting access and processing to necessary purposes. GDPR aims to balance innovation and privacy, empowering individuals with informed choices and protecting their rights amidst evolving digital landscapes.

Under the GDPR, data processors share responsibility for specific activities, although ultimate responsibility typically lies with the data controller, and the processor's obligations are governed by a contract defining processing activities and methods for handling personal data, primarily entailing adherence to lawful instructions from the controller.[53] To be more specific, processors must uphold confidentiality by limiting data access to authorized personnel.[54] They are also obligated to maintain detailed records of processing activities for transparency and accountability.[55] In addition, both processors and controllers implement technical and organizational measures to protect data.[56] Processors assist controllers in meeting GDPR obligations[57] and promptly notify them of any data processing changes or incidents.[58]

46 Recital 61 of the GDPR.
47 Orla, L. (2023), 'Complete and effective data protection', *Current Legal Problems*, Vol. 76, p. 300.
48 Article 5 of the GDPR.
49 Article 5(1)(b-f) of the GDPR.
50 Recital 64 and Article 12 of the GDPR.
51 Tobias, N. (2023), *supra* note 2, p. 215.
52 Article 25 of the GDPR.
53 If the processor fails to comply with these obligations or acts against the controller's lawful instructions, they can be held liable or fined, according to Article 28(4), GDPR.
54 Article 28(3) of the GDPR.
55 Article 30(2) of the GDPR.
56 Article 32 of the GDPR.
57 Article 28(3) of the GDPR.
58 Article 33(2) of the GDPR.

According to the mutual obligation between the controller and processor, it is mandatory to appoint a data protection officer in certain cases. These include:[59] (i) when a public authority or body, excluding courts acting in their official capacity, processes data on their behalf; (ii) when the controller or processor carries out large-scale processing operations that involve frequent and systematic monitoring of data subjects; and (iii) when the controller or processor processes special categories of data as outlined in Article 9 of the GDPR, as well as personal data related to criminal convictions and offences mentioned in Article 10 of the GDPR. In case of other than those referred, controller and processor may designate a data protection officer for the reason of representing[60] and acting for regulated tasks regarding Article 39 GDPR.[61]

Regarding the mechanism of non-personal data, especially in the context of connected products, the principles of fairness and contractual freedom are highlighted as governing the relationship between data users and data holders.[62] When a connected product's manufacturer is a data holder, a contract between the manufacturer and the user should serve as the legal foundation for the manufacturer's use of non-personal data.[63] Data holders should not share non-personal data with third parties beyond their contract with the user, unless required by law. In contrast, users of connected products can share data easily, including for business purposes.[64] Consumer protection laws apply to contracts between data holders and consumers using connected devices to protect against unfair commercial conditions.[65] Thus, it can be seen that the relationship amongst actors involved in non-personal data transmission is considered as relationship between data controllers. This sense follows the fact that the obligations of data user, data holders and third parties listed in Regulation 2023/2854 closely resemble obligations of data controllers, as follows: obligation to make data accessible,[66] the obligation to make data available product data and related service data from data holders to users,[67] obligation of third party recipient[68] (integrity and confidentiality), and contractual obligation amongst parties.[69]

59 Article 37 of the GDPR.
60 Article 37(4) of the GDPR.
61 Article 39 of the GDPR.
62 Recital 43 of the Regulation 2023/2854.
63 Recital 25 of the Regulation 2023/2854.
64 Recital 26 of the Regulation 2023/2854.
65 Recital 28 of the Regulation 2023/2854.
66 Article 3 of the Regulation 2023/2854.
67 Article 4 of the Regulation 2023/2854.
68 Article 6 of the Regulation 2023/2854.
69 Recital 74 of the Regulation 2023/2854.

Hence, in cross-border data transmission, key actors must use technical tools and legal measures to safeguard against cyber-attacks and ensure compliance with data protection principles. This includes security by design and encryption methods, ensuring efficient and secure data transfers for business purposes. Controllers must notify any elements that may identify personal data, such as embedded tools on websites, to maintain protection standards.

1.3. Remedies for violations of data transmission regulation

As one of the processing methods prescribed in GDPR, the violation of data transmission concerns the behavior of controllers and processors as the main key actors involved. Article 83 of the GDPR outlines infringements of data transmission based on certain criteria.

First, the purpose of data transmission is the initial factor which aims to facilitate the methodology for data providers and recipients to get access to decisive data.[70] However, if this process results in accidental or unlawful breaches of personal data – such as destruction, loss, alteration, unauthorized disclosure, or access – it contradicts the intended goal of data transmission,[71] resulting in a violation of data transmission principles, compromising the integrity and security of the data exchanged.

Second, the behavior of the controller and processor is also a determinant, which is guided by various indications, including their intentions, efforts to mitigate risks, responsibilities, previous infringements, and their adherence to regulations.[72] The GDPR mandates fair and transparent data management by controllers and processors, ensuring compliance with the Regulation. Their behavior must be properly monitored to enforce adherence to data protection standards.

Third, the severity of data breaches determines the legal consequences and sanctions under the GDPR, categorized into two levels: involvement of supervisory authorities and factors aggravating or mitigating the breach. Recital 148 emphasizes enhancing GDPR enforcement through penalties, including administrative fines, imposed by supervisory authorities for breaches of the GDPR norms.[73] Recital 148 also indicates that the code of conduct and any other aggravating or mitigating factor are objectives required to adhere to, as well as other prescribed factors, constitutes the infringement of GDPR.[74] Data breaches in transmission involve controllers, processors, and supervisory authorities, leading to legal actions

70 Article 83(2)(a) of the GDPR.
71 Article 4(12) of the GDPR on the definition of personal data breach.
72 Article 83(2)(a), (b), (c), (d), (e), (j) of the GDPR.
73 Recital 148 of the GDPR.
74 Recital 148 of the GDPR.

against controllers and processors and challenges to supervisory authority decisions. Data subjects can seek legal remedies against both, unlike the Data Protection Directive, which only included controllers.[75] Additionally, everyone has the right to a strong legal defense if a supervisory authority issues legally binding decisions against them,[76] excluding advisory opinions or non-binding rulings. [77]

Violation of non-personal data transmission occurs when there is a breach of the agreement governing the transfer process, which hinges on consent from data holders, recipients, controllers, and processors. It encompasses inadequate disclosure, misuse,[78] and unauthorized movement of data.[79] Remedies for these violations primarily address business interactions and aim to compensate damages fairly. Such breaches can lead to loss of data quantity or quality, affecting contractual relationships. Additionally, compromised confidentiality and information integrity can harm economic activities, potentially resulting in financial losses.[80] Therefore, compensatory damages are crucial in resolving non-personal data transmission issues and ensuring accountability in data handling practices.

2. *Status quo* of Vietnam's regulation of data transmission in comparison with that of the European Union

Vietnam is advancing digital transformation with policies supporting technology development and a legal framework.[81] It addresses both data protection and the free flow of data through Decree No. 13/2023/ND-CP on personal data protection and the 2023 Law on Electronic Transactions, aiming to regulate data exchanges in economic activities while preventing illegal trading of personal data without consent. Data transmission in Vietnam is defined by legal provisions such as the 2006 Law on Information Technology,[82] the 2023 Law on Electronic Transactions,[83] and Decree No. 13/2023/ND-CP,[84] emphasizing its role in digital technology and facilitating the unrestricted movement of data, including personal data, in various contexts.

Vietnamese data transmission regulation has two objectives: enabling electronic transactions and protecting personal data. Transmission involves

75 Article 79 of the GDPR.
76 Article 77 of the GDPR.
77 Recital 143 of the GDPR.
78 Article 3 of the Regulation 2023/2854.
79 Article 6 of the Regulation 2023/2854.
80 Recital 31 of the Regulation 2023/2854.
81 Article 3(4) of the Decree No. 13/2023/ND-CP.
82 Article 16 of the 2006 Law on Information technology.
83 Article 3(2) of the 2023 Law on Electronic transaction.
84 Article 2(7) of the Decree No. 13/2023/ND-CP.

two parties: the originator, who is considered a controller as they create and send data[85] and the recipient.[86] The controller[87] and processor[88] is an entity that simultaneously decides the purpose, means, and directly processes personal data. In essence, the originator of data is considered a controller, as data is created and sent by the originator before it has been stored.[89] This is similar to the definition of controller for self-decisive purposes and means of processing data.[90] Other parties receiving the data must clarify their usage or purpose by agreement.[91]

Decree No. 13/2023/ND-CP, similar to the GDPR, mandates transparency,[92] notification, and information provision to data subjects,[93] including data modification and breach notifications.[94] It requires the fair handling of personal data, including storage, deletion, or destruction with the subject's acknowledgment.[95] For data transferred abroad, controllers and processors must maintain records assessing the impact of processing and transferring personal data from the start, ensuring compliance for inspections, investigations, and assessments by authorities.[96] This approach underscores Vietnam's commitment to data privacy amid evolving regulatory challenges.

Notably, Vietnamese regulation does not define the concept of a joint controller. The only group of transmitting actors mentioned is the intermediary element, as outlined in Article 16 of the 2006 Law on Information Technology.[97] This absence might potentially lead to ambiguity or gaps in accountability and responsibility between parties involved in data transmission activities, as Vietnamese law may not provide adequate guidance on how responsibilities should be allocated and coordinated among multiple entities involved in data processing.

Besides, Vietnamese legislation addresses personal data protection violations in privacy, confidentiality, and telecommunications. Three forms of remedies are mandated: civil, administrative, and criminal. Civil remedies include contractual sanctions or compensation for damages. Decree No. 15/2020/ND-CP outlines administrative sanctions in postal,

85 Article 14 of the 2023 Law on Electronic transactions.
86 Article 16 of the 2023 Law on Electronic transactions.
87 Article 9 of the Decree No. 13/2023/ND-CP.
88 Article 10 of the Decree No. 13/2023/ND-CP
89 Article 14 of the 2023 Law on Electronic transactions.
90 Article 2(9) of the Decree No. 13/2023/ND-CP.
91 Article 16 of the 2023 Law on Electronic transactions.
92 Article 11 of the Decree No. 13/2023/ND-CP.
93 Article 12(3), Article13, and Article 14 of the Decree No. 13/2023/ND-CP.
94 Article 23 of the Decree No. 13/2023/ND-CP.
95 Article 16 of the Decree No. 13/2023/ND-CP.
96 Article 24 and Article 25 of the Decree No. 13/2023/ND-CP.
97 Article 16 of the 2006 Law on Information technology.

telecommunications, radio frequencies, IT, and electronic transactions, with possible penalties including fines and remedial actions.[98]

Overall, the regulation of data transmission in Vietnam has recently evolved toward the universal personal data protection principles and those of the GDPR. However, Vietnam's lack of detailed definitions for non-personal, anonymized, or pseudonymized data creates ambiguity and increases exposure risks.[99] The concept of a joint controller is also unclear, with no provisions addressing it. Thus, Vietnam's data transmission regulation aims to safeguard personal data but falls short in addressing the identification of data and the roles of data holders and users when transmission does not involve personal data.

3. Recommendations for Vietnam from European Union experience

First, the regulation of data transmission in Vietnam should expand to include key aspects such as defining non-personal data, joint controllership, data holders, and data users. The status of joint controller is not automatically assigned to parties using a shared data processing system. This is especially true if one party can handle the data independently or if the provider processes the data solely on behalf of the parties without a separate objective.[100] The allocation of responsibility to each controller in the event of conflict is unambiguous, hence facilitating the resolution of disputes.

Second, Vietnamese regulations propose compensation and penalties for data transmission violations, focusing on telecommunications and commerce. However, the lack of comprehensive legal recourse complicates managing personal data misuse and attribution.[101] Therefore, the EU's regulation on remedies for data transmission violations is worth pondering for Vietnam in order to enhance and refine its own legal measures in this area.

Third, it is necessary to enhance the mechanism for stricter monitoring of compliance by the data controller and processor in cross-border data transmission. Establishing a data protection officer role, as per GDPR, could bolster regulatory oversight and advance Vietnamese data transmission regulations. ●

98 Ly N. H. (2020), 'Pháp luật hiện hành của Việt Nam về bảo vệ dữ liệu, thông tin cá nhân và quyền riêng tư' [Vietnam's laws on the protection of personal data, personal information, and privacy]. Retrieved from: https://nacis.gov.vn/nghien-cuu-trao-doi/-/view-content/214123/phap-luat-hien-hanh-cua-viet-nam-ve-bao-ve-du-lieu-thong-tin-ca-nhan-va-quyen-rieng-tu [accessed 30 April 2024].

99 Lederer, S., Hong, J. I., Dey, A. K, et al. (2004), 'Personal privacy through understanding and action: Five pitfalls for designers', *Personal and Ubiquitous Computing*, Vol. 8, p. 441.

100 European Data Protection Board (2021), *supra* note 44.

101 Ministry of Information and Communications (2021), 'Chế tài xử lý hành vi vi phạm quy định bảo vệ dữ liệu cá nhân' [Sanctions for violations of personal data protection regulations]. Retrieved from: https://mic.gov.vn/che-tai-xu-ly-cac-hanh-vi-vi-pham-quy-dinh-bao-ve-du-lieu-ca-nhan-197149685.htm [accessed 30 April 2024].

References

**** Cases***

[1] *Joined Cases C-293/12 and C-594/12*, EU Court of Justice (8 April 2014)

[2] *Case T-557/20*, EU Court of Justice (26 April 2023)

[3] *Case C-131/12*, EU Court of Justice (13 May 2014)

[4] *Case C-101/01*, EU Court of Justice (6 November 2003)

**** Books and Articles***

[5] European Data Protection Board (2023), *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, Version 2.0

[6] Lederer, S., Hong, J. I., Dey, A. K, et al. (2004), 'Personal privacy through understanding and action: Five pitfalls for designers', *Personal and Ubiquitous Computing*, Vol. 8

[7] Ly N. H. (2020), 'Pháp luật hiện hành của Việt Nam về bảo vệ dữ liệu, thông tin cá nhân và quyền riêng tư' [Vietnam's laws on the protection of personal data, personal information, and privacy]. Retrieved from https://nacis.gov.vn/nghien-cuu-trao-doi/-/view-content/214123/phap-luat-hien-hanh-cua-viet-nam-ve-bao-ve-du-lieu-thong-tin-ca-nhan-va-quyen-rieng-tu [accessed 30 April 2024].

[8] Margaret, R. (2023), 'What does data transmission means?'. Retrieved from: https://www.techopedia.com/definition/9756/data-transmission [accessed 30 April 2024]

[9] Michèle, F., and Frank, P. (2020), 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law*, Vol. 10, No. 1

[10] Orla, L. (2023), 'Complete and effective data protection', *Current Legal Problems*, Vol. 76,

[11] Raphaël, D. (2020), 'Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?', *Regulation & Governance*, Vol. 16, No. 1

[12] Tim, H. (2020), 'Sharing is caring – Date sharing initiatives in healthcare', *International Journal of Environmental Research and Public Health*, Vol. 17, No. 9

[13] Tobias, N. (2023), 'The restrictive effect of the legal mechanism for data transfers in the European Union', in: Tobias, N. (2023), 'Data protection without data protectionism', *European Yearbook of International Law*, Vol. 28

Author Contribution

All authors contributed to the study conception and design. All authors read and approved the final manuscript.

Declarations

Conflict of Interest: The authors declare no competing interests.

Disclaimer: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.