REVIEW ARTICLE

AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Review Article

POTENTIAL CONFLICTS IN PERSONAL DATA PROTECTION UNDER CURRENT LEGISLATION IN VIETNAM COMPARED WITH EUROPEAN GENERAL DATA PROTECTION REGULATION

Hoa Thanh Ha and Tuan Van Vu*

ABSTRACT

Background: *Transatlantic data transfers are a critical component of the global digital economy, facilitating commerce and communication among countries worldwide. However, these transfers have been fraught with legal and regulatory challenges, particularly concerning protecting personal data due to the lack of a comprehensive global privacy law.*

Methods: *This comparative, descriptive study exploits secondary resources by comparing and contrasting the principles of the European General Data Protection Regulation and the new Decree on personal data protection in Vietnam to provide deep insights into the differences between them.*

Results and Conclusions: *Although the Decree takes advantage of many of the European General Data Protection Regulation's principles, i.e., the rights of data subjects, consent requirements, and the need for impact assessments, it has its provisions specific to the Vietnamese context, such as the absence of "legitimate interests" as a legal basis for processing and the unique enforcement mechanisms. Despite many similarities, the specific requirements around consent, data subject rights, breach notification, extraterritorial data transfers, and enforcement mechanisms might result in conflicts among these legislative documents. The Decree, which would become more effective, shall rely on its enforcement mechanisms and the ability to impose meaningful sanctions for non-compliance; thus, it should incorporate a more detailed sanctions regime to deter violations effectively.*

.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

1 INTRODUCTION

Transatlantic jurisdictional conflicts regarding privacy and personal data protection have emerged as growing global concerns worldwide. The increased reliance on the Internet and e-commerce activities has prompted countries to enact data privacy laws to safeguard individuals' personal data. However, the situation where there is a lack of one comprehensive international privacy law governing personal data protection worldwide[1] necessitates a global legal instrument to establish a common unified framework for lawfully collecting, using, and storing the personal data of individuals.[2] Currently, personal data protection is counted as a relatively new field of laws which has been constructed and developed within certain countries or regions.[3]

Unfortunately, since no single supervising authority is in charge of enforcing a comprehensive international regulatory framework, States must individually legislate and implement their own legislative regulations to address the issue of personal data protection, which directly affects transatlantic privacy data. Besides, differences in transatlantic regulations are likely to create legal hindrances for multi-jurisdictional businesses to comply with potentially conflicting rules.[4] Due to the rapid global integration, personal information sharing and use occur across national borders. It is consequently impossible to adequately protect citizens' privacy data within a country's borders. In this regard, data privacy protection can be seen as an international issue that needs harmonisation and comprehensive solutions to be regulated by the world privacy laws applicable within certain countries or regions.[5]

1 Alsamara Tareck, 'Legal Mechanisms for the Stimulation of the Digital Economy in Developing Countries' (2023) 6(Spec) Access to Justice in Eastern Europe 72, doi:10.33327/AJEE-18-6S002.

2 Florent Thouvenin and Aurelia Tamò-Larrieux, 'Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market?' in M Burri (ed), *Big Data and Global Trade Law* (CUP 2021) 316, doi:10.1017/9781108919234.020.

3 Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the US and the EU?' (2020) 8(1) Penn State Journal of Law & International Affairs 49.

4 Giovanni Comandè and Giulia Schneider, Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think' (2022) 23(4) German Law Journal 559, doi:10.1017/glj.2022.30; Giovanni de Gregorio, 'The Transnational Dimension of Data Protection: Comparative Perspectives from Digital Constitutionalism' (2022) 1(2) The Italian Review of International and Comparative Law 335, doi:10.1163/27725650-01020006; Peter J van de Waerdt, 'Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market' (2020) 38 Computer Law & Security Review 105436, doi:10.1016/j.clsr.2020.105436.

5 Gregorio (n 4); M Bas Seyyar and Zjmh Geradts, 'Privacy impact assessment in large-scale digital forensic investigations' (2020) 33 Forensic Science International: Digital Investigation 200906, doi:10.1016/j.fsidi.2020.200906; Mistale Taylor, 'Limits that Public International Law Poses on the European Union Safeguarding the Fundamental Right to Data Protection Extraterritorially' in M Taylor, *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality* (CUP 2023) 57, doi:10.1017/9781108784818.004.

The need to establish a comprehensive international data privacy law has caused a longstanding debate and many challenges.[6] This is because the differing legal approaches to personal data protection laws in effect in different countries or regions need to comply with a feasible international privacy law. The current situation shows that 71 per cent of the countries have adopted their data protection and privacy legislation while 9 per cent have drafted their own. Remarkably, 15 per cent of the countries have no legislation for data protection and privacy law, whereas 5 per cent have no data for this kind of legislation.[7] From the previous figures, it is notable to recognise that international regulations on data privacy protection have gained greater attention all over the world. States have promulgated their own data privacy laws to supply sufficient protections for personal transatlantic exchanges.

A lack of international regulatory framework results in the different data privacy laws across the world, which proves the incident that the law of personal data protection in one country possibly provokes a direct legal conflict with one another in international data transfers due to contradictory scopes of the privacy data laws; thus, this divergence causes legal ambiguity and gaps in privacy protections.[8] In addition, some countries have yet to legitimise data privacy laws or have not seriously taken legal personal data protection issues into consideration. These formidable obstacles call for the legal adequacy requirement for transatlantic data, only settled by a single supervisory authority that enforces a comprehensive international data privacy law.[9]

Although there is no single regulatory instrument addressing personal data protection on an international scale, some prominent examples of privacy laws have significant features applicable within certain countries or regions.[10] For instance, the European-style General Data Protection Regulation (hereinafter the GDPR)[11] in the European Union (EU) embraces the critical concept that protecting personal data implements a basic right. According to Art. 8(1) of the Charter of Fundamental Rights of the European Union (the

6 Mistale Taylor, 'Data Protection and the Free Flow of Information' in M Taylor, *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality* (CUP 2023) 150, doi:10.1017/9781108784818.007.

7 'Data Protection and Privacy Legislation Worldwide' (*UN Trade & Development - UNCTAD*, 2024) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 10 March 2024.

8 Gregorio (n 4).

9 Patrik Hummel, Matthias Braun and Peter Dabrock, 'Own Data? Ethical Reflections on Data Ownership' (2020) 34 Philosophy & Technology 545, doi:10.1007/s13347-020-00404-9.

10 Comandè and Schneider (n 4); Paul Quinn and Gianclaudio Malgieri, 'The Difficulty of Defining Sensitive Data - The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22(8) German Law Journal 1583, doi:10.1017/glj.2021.79.

11 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) (GDPR) [2016] OJ L 119/1 <http://data.europa.eu/eli/reg/2016/679/oj> accessed 10 March 2024.

'Charter')[12] and Art. 16(1) of the Treaty on the Functioning of the European Union (TFEU),[13] these legal normative regulations stipulate that each legal person endows the right to the personal data protection.[14]

In contrast, personal data is likened to a commodity in the market under the Privacy Act of 1974 in the United States,[15] and its focal notion concentrates on policing fairness in exchanges of personal data.[16] In contrast, China's Personal Information Protection Law (PIPL)[17] is deeply rooted in the legal transplantation of both the US and the EU reference models but incorporates distinctive features. The PIPL emphasises protecting individuals' rights against private entities while simultaneously enhancing government access to personal data. In simple terms, privacy protection is determined by individuals' rights.[18]

Meanwhile, remarkably, given the recent situation in Vietnam, the Government has enacted the long-awaited Decree No.13/2023/ND-CP (hereafter the Decree)[19] on personal data protection. This constitutes the first-ever consolidated and comprehensive legal instrument for collecting and processing personal data in Vietnam and officially came into effect on 1 July 2023.

For the corpus of this paper, the extent of the Decree will be examined to contrast and compare with one of the international privacy laws currently taking effect in the European Union, namely the GDPR issued on 27 April 2016 and the regulation on 25 May 2018.[20] Data privacy laws (personal data protection laws used interchangeably in this article) are considered emerging fields of laws worldwide. In exploring the data privacy interoperability between the Decree and GDPR, this study compares and contrasts the respective legal identities legitimised for protecting personal data in Vietnam and the EU.

12 Charter of Fundamental Rights of the European Union (2012/C 326/02) [2012] OJ C 326/391 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:C2012/326/02&qid=1715593591875> accessed 10 March 2024.

13 Treaty on the Functioning of the European Union (TFEU) [2016] OJ C 202/47 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=legissum:4301854> accessed 10 March 2024.

14 Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106(1) Georgetown Law Journal 123.

15 US Department of Justice, *Overview of the Privacy Act of 1974* (2020 edn) <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition> accessed 10 March 2024.

16 Schwartz and Peifer (n 14) 127.

17 Personal Information Protection Law of the People's Republic of China of 20 August 2021 (PIPL) <https://personalinformationprotectionlaw.com/> accessed 10 March 2024.

18 Pernot-Leplay (n 3); 'The China Personal Information Protection Law (PIPL)' (*Deloitte,* May 2021) <https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html> accessed 10 March 2024.

19 Decree of the Government of the Socialist Republic of Vietnam no 13/2023/ND-CP of 17 April 2023 'On Personal Data Protection' (Decree no 13/2023/ND-CP) <https://english.luatvietnam.vn/decree-no-13-2023-nd-cp-dated-april-17-2023-of-the-government-on-personal-data-protection-249791-doc1.html> accessed 10 March 2024.

20 GDPR (n 11).

This research also emphasises noticeable differences between the two legal systems addressing the newly appearing issues of data privacy laws. In particular, this study employs a qualitative method of a descriptive comparative research design to reflect the potential of the two legal systems to seek mutually acceptable standards of data privacy protection. To overcome the potential jurisdictional disputes over Vietnam - EU data privacy interoperability, both the Decree and GDPR have to be harmonised to align more with mutual international standards of practical personal data processing activities. Consequently, the future of transatlantic data between the two systems of data privacy law, Vietnam and the EU, has to acquire a profound understanding of protecting personal data within these new respective structures.

2 METHODS AND MATERIALS

The study used a qualitative approach to theoretically synthesise, analyse, and compare the secondary sources following a recent model introduced by Long-Sutehall[21] about addressing a secondary analysis of primary qualitative datasets. The research compared the new Decree on personal data protection in Vietnam and the EU's General Data Protection Regulation 2016/679 to determine if any potential conflicts exist in implementing these legal normative documents in practice. The legally incompatible authorities of these Regulations would be for the interests of data subjects who have to go between these two influential jurisdictions.

3 OVERVIEW OF THE NEW DECREE ON PERSONAL DATA PROTECTION IN VIETNAM AND THE EU'S GENERAL DATA PROTECTION REGULATION 2016/679

3.1. Key takeaways from Vietnam's Personal Data Protection Decree 2023[22]

Until 17 April 2023, Vietnam had a fragmented legal framework for regulating personal data protection governed by 19 laws and regulations. Recognising the need for a more cohesive approach, the government issued a draft on 9 February 2021, which underwent several revisions before the official promulgation of the Decree of Personal Data Protection (the Decree). In the short term, the Decree is a foundational step towards future legislation and aims to consolidate existing laws and regulations into a comprehensive and uniform framework for safeguarding individuals' data.

Although regarded as having a lower legal status in Vietnam's statutory hierarchy compared with laws and codes, the Decree has significant impacts on the regulation of

21 Tracy Long-Sutehall, Magi Sque and Julia Addington-Hall, 'Secondary Analysis of Qualitative Data: A Valuable Method for Exploring Sensitive Issues with an Elusive Population' (2010) 16(4) Journal of Research in Nursing 335, doi:10.1177/1744987110381553.

22 Decree no 13/2023/ND-CP (n 19).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

personal data protection in the current situation in Vietnam as personal data protection characterises a new and developing legal regulation. Despite its inferior status, this first comprehensive legislative instrument on personal data protection regulates all activities regarding personal data protection. In the event of those who disrespect any provisions of the Decree, they might receive some forms of punishment from its legal enforcement.

The Decree prescribes the important obligations of agencies, organisations, and individuals to comply with the regulations prescribed by the Decrees in accordance with the merits they receive thereof. Compared with the GDPR, the Decree characterises exclusive provisions designated to fit into only Vietnam's context. For example, Art. 3(4) stipulates that "collected personal data must be appropriate and within the scope and purposes of processing. Purchase and sale of personal data in any form shall not be permitted, unless otherwise provided by law".[23] According to this rule, the commodification of personal data is strongly prohibited, and those committing this activity without conformity with the law confront severe legal consequences. Moreover, Art. 3 points out that the data subjects have the right to be informed about activities concerning his/her personal data processing, which connotes the fact that without their consent any action such as personal data collection, transfer, or purchase thereof, unless otherwise provided by law, is regarded as the violation of the Decree and must be in charge of relevant legal litigation.

Similarly, Art. 2(9-10) declares that a controller refers to an organisation or individual deciding the purposes and means of personal data processing. Similarly, a processor denotes an organisation or individual processing personal data under the supervision of the controller; he/she enters into a contract or agreement with the controller. In a sense, the Decree recognises the roles of Personal Data Controllers and Personal Data Processors as separate entities. This legal distinction between the two categories has made the Decree unique and different from other data protection laws worldwide. Although a lack of classification between Personal Data Controllers and Processors possibly leads to clarity and precision in determining the liabilities and unity of different subjects in terms of personal data processing, privacy laws might accumulate more unnecessary complexity because of the overlapping conceptual distinction between Personal Data Controller and a Personal Data Processor. As a result, the inclusion of both aforementioned entities causes much difficulty in navigating and harmonising the requirements of transboundary privacy laws.

Another remarkable difference is how the Decree specifies a general provision for those who violate its regulations. Based on the level of violation of the Decree, respective punishments are given to violators, such as disciplinary action, administrative penalties, or criminal prosecution, which is outlined in Art. 4. Astonishingly, while some States in the EU and the US empower their own independent personal data protection

23 ibid, art 3(4).

commission to govern the enforcement of the Privacy Act,[24] the Decree is vested its authority by the Government which shall perform the uniform state management of personal data protection (as stated in Art. 5) under the control of an existing agency within the Ministry of Public Security (MPS), the Department of Cyber Security and Hi-tech Crime Prevention (A05).

Art. 1(2.d) addresses foreign agencies, organisations, and individuals directly engaged in or related to processing personal data in Vietnam, subjecting them to regulation under the Decree. However, this provision raises questions about the extent of foreign involvement in personal data processing activities and requires more clarification regarding the specific aspects and scope of regulation applicable to foreign agencies. Otherwise, this legal ambiguity will likely put many third-party service providers or software vendors at risk in terms of violating the limitation of personal data processing involvement as outlined in Art. 2(12).

Remarkably, the Decree clearly defines the nature of personal data as prescribed in Art. 2(1). It prescribes that "Personal data means any information in the forms of symbols, letters, figures, images, sounds or similar forms in the electronic environment that is associated with a particular person or may lead to the identification of a particular person. Personal data includes basic personal data and sensitive personal data."[25] Expanding on the above rule, Art. 2(1) mentions two typical terms, namely basic personal data and sensitive personal data. In particular, two terms in Art. 2 are defined as follows:

"*3. Basic personal data includes:*

a) Family name, middle name, and first name as stated in a birth certificate, other name (if any);
b) Date of birth; date of death or missing;
c) Gender;
d) Place of birth, place of birth registration, place of permanent residence, place of temporary residence, current place of residence, native place, contact address;
dd) Nationality;
e) Image of the individual;
g) Telephone numbers, people's identity card numbers, personal identification numbers, passport numbers, driver's license numbers, numbers on vehicles' number plates, personal tax identification numbers, social insurance numbers, health insurance card numbers;
h) Marital status;
i) Information about family relationships (parents, children);
k) Information about the digital account of the individual; personal data on activities, history of activities in cyberspace;

24 Pernot-Leplay (n 3).

25 Decree no 13/2023/ND-CP (n 19) art 2(1).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

l) Other information associated with a particular person or leading to the identification of a particular person, other than those specified in Clause 4 of this Article.

4. Sensitive personal data means any personal data associated with an individual's privacy rights of which the violation directly affects his/her lawful rights and interests, including:

a) Political opinions, religious opinions;
b) Health status and private information recorded in the health record, excluding the information about blood type;
c) Information relating to racial origin, ethnic origin;
d) Information about the inherited or acquired genetic characteristics of the individual;
dd) Information about physical characteristics, and unique biological characteristics of the individual;
e) Information about the sex life, and sexual orientation of the individual;
g) Data on crimes and offenses are collected and stored by law enforcement authorities;
h) Client information of credit institutions, foreign bank branches, intermediary payment service providers, and other authorized organisations, including client identification information prescribed by law provisions, information on accounts, deposits, deposited assets, transactions, organisations and individuals being securing parties at credit institutions, bank branches, intermediary payment service providers;
i) Location data of the individual identified through location services;
k) Other personal data being particular and requiring necessary security measures under law provisions."[26]

According to the Decree, more stringent protection measures for sensitive personal data than for basic personal data shall be implemented to avoid the possibility of the sale or purchase of personal data. For example, in processing any sensitive personal data, unless otherwise provided by law, regulated agencies must inform data subjects about the processing of their sensitive personal data and obtain explicit consent from them. Accordingly, organisations that are disciplined by the Decree have to set up a department in charge of processing and supervising the protection of sensitive personal data within their organisations and these departments are closely collaborated with the A05 in all situations. It cannot be denied that the Decree on Personal Data Protection in Vietnam has a far-reaching consequence in protecting personal data and marks a historic milestone for a more comprehensive, internationalised, stringent law in the coming time.

Currently, the Decree not only sets out the essential concepts and principles of personal data protection but also introduces specific provisions for data processors and controllers. It also establishes a legal framework for obtaining consent regarding data processing activities, transboundary data transfers, and child data protection. This may ensure privacy and provide stricter security of individuals' data.

26 ibid, art. 2.

In practice, the present legal enforcement of the Decree has been in effect and gained some achievements to handle many of the current serious challenges in terms of confronting personal data protection in Vietnam; however, it still contains significant legal loopholes that call for more actions to be dealt with in forthcoming time via directives, circulars or joint-circulars. It fails to stipulate any specific procedure for addressing complaints about the violations of personal data protection. Furthermore, the Decree must clarify the conflicting provisions on the sale of personal data.

As stated in Art. 4, handling a breach of personal data protection regulation stipulates that "agencies, organisations, and individuals breaching the personal data protection regulation shall, depending on the seriousness of their breaches, be disciplined, administratively or criminally handled in accordance with regulations."[27] As such, the Decree does not clarify the principles for settling conflicts on personal data privacy violations. In addition, the Decree has to be supplemented with regulations regarding the impact of transboundary data transfers together with transparent guidelines and requirements for such transfers and greater clarity on transatlantic activities.

At present, the Vietnamese government prioritises digital transformation to simplify all procedures and cut down on administrative procedures handled directly by humans. This means that more security shall be assigned to biometric data; thus, the Decree should revise its provisions to consider the issue of biometric data. In other words, guidelines on automated processing shall be provided, and statutory regulations for biometrics shall also be constituted.

Decision No. 749/QD-TTg 2020 on approving the national digital transformation program through 2025, with orientations toward 2030 by the Prime Minister firmly asserts that the utmost priority shall be given to three pillars: digital government, digital economy, and digital society, in which the strategy of "moving to the cloud" is seen as the most important factor to help enterprises develop in a digital economy.[28] For this reason, the Decree should be revised to tackle growing issues such as automated personal data processing, biometrics or facial recognition, transatlantic personal data transfer, and protected digital cross-border business activities.

The rapid advancement of the Industrial Revolution (IR) 4.0 in Vietnam, as reported by the International Labour Organisation (ILO)[29] - Country Office for Vietnam,

27 ibid, art. 4.

28 Decision of the Prime Minister of the Socialist Republic of Vietnam no 749/QD-TTg 2020 of 3 June 2020 'On Approving the National Digital Transformation Program Through 2025, with Orientations Toward 2030' <https://english.luatvietnam.vn/decision-no-749-qd-ttg-on-approving-the-national-digital-transformation-program-until-2025-with-a-vision-184241-doc1.html> accessed 10 March 2024.

29 ILO, 'Industrial Revolution (Ir) 4.0 in Viet Nam: What Does it Mean for the Labour Market?: Policy brief' (*International Labour Organisation - ILO*, 30 May 2018) <https://www.ilo.org/publications/industrial-revolution-ir-40-viet-nam-what-does-it-mean-labour-market> accessed 10 March 2024.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

underscores the importance of Vietnam's commitment to personal data protection and privacy. A robust personal data protection framework in Vietnam is essential for its successful integration into the global economy, ensuring compliance with privacy laws in the region and around the world.

3.2. Overview of the EU's General Data Protection Regulation (GDPR) 2016/679[30]

One of the most influential, effective, and statutory resolutions has geographically shown tremendous power over privacy laws in European countries. Since GDPR became effective on 25 May 2018, it has been regarded as the strongest legislative instrument of data protection rules worldwide. It instructs how individuals can control their personal information and determines to what extent organisations can process their personal data.

The GDPR comprises 11 chapters, containing 99 individual articles therein as a result of long-planned data protection reforms to undergo more than four years of extensive discussions and lengthy negotiations to commonly promulgate the GDPR's final framework for laws across the European continental countries.[31] The European Parliament and European Council officially adopted the GDPR in April 2016, which was enforced around two years later across Europe to modernise the laws that protect individuals' privacy laws. The GDPR was generated, standardised, and compromised data privacy laws among European countries to secure greater legal protection and rights for individuals. The GDPR's legislative authority includes more disciplinary sanctions to regulate how businesses and other agencies can address the information of those who involve them.

The crucial element that functions as the heart of the GDPR is personal data protection, precisely referring to the four factors that centralise all the legislative measures. The four fundamental data subjects are clearly defined as data controllers (Art. 4.7), data processors (Art. 4.8), recipients (Art. 4.9), and third parties (Art. 4.10) of the GDPR. The details of the four key elements mentioned above are specified in Chapter 3, Chapter 4, and Chapter 6 of the GDPR.

Firstly, regarding the data subject's rights, these regulations are grouped in Chapter 3, including five sections with twelve articles. The rights of the data subject enshrined in this chapter are greatly renewed in terms of how personal data regulations are addressed. It encompasses eight principal data subject rights in addition to the right to

30 GDPR (n 11).

31 Michèle Finck, 'Hidden Personal Insights and Entangled in the Algorithmic Model: The Limits of the GDPR in the Personalisation Context' in U Kohl and J Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law* (CUP 2021) 95; Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) Information & Communications Technology Law 65, doi:10.1080/13600834.2019.1573501; Schwartz and Peifer (n 14).

withdraw consent which empowers individual autonomy over personal data and as well as data processing as follows:

- *Right to be informed* (Arts. 12-14): Data subjects are informed about the collection and purpose of using personal data according to these regulations. In particular, they have the right to know the purpose of data processing, the retention length, and other specified rights granted to them accordingly.
- *Right to access* (Art. 15): Data subjects have the right to request and receive a copy of their personal data and information about the aims and the extent of their personal data from one organisation addressing their personal data.
- *Right to rectification* (Art. 16): Data subjects have the right to request to correct or update their inaccurate or outdated personal data held by an organisation.
- *Right to be forgotten/ Right to erasure* (Art. 17): Data subjects have the right to request their personal data be removed in some situations. However, the deletion of their personal data characterizes no absolute rights as it is subject to exemptions depending on some situations.
- *Right to data portability* (Art. 20): Data subjects have the right to request that their personal data be transferred to another controller or receive it in a structured, normally used, and machine-readable format. The data is surely in machine-readable electronic format.
- *Right to object* (Art. 21): Data subjects have the right to object to the processing of their personal data, especially for the purpose of direct marketing. It is unlawful for an organization to continue processing data if it cannot provide legitimate grounds for processing the personal data for the sake of the interests, rights, and freedoms of the data subject.
- *Right to object to automated processing* (Art. 22): Data subjects have the right to overrule any decision made solely with their data based on automated decision-making or profiling. Accordingly, they have the right to call for human intervention to give their viewpoints and take responsibility for their decision.
- *Right to restrict processing* (Arts. 18 and 23): Data subjects have the right to request to restrict or suppress the processing of their personal under some circumstances.

Secondly, the framework for the roles, obligations, and responsibilities of data controllers and data processors is comprehensively stipulated in Chapter 4 of the GDPR. Data controllers and data processors are structured into five sections concentrating on the necessity of obeyance the regulation, the need for data security, the data protection impact assessment and prior consultation, the legal requirements for data protection officers, and the mandatory compliance and significant penalties for non-compliance of ensuring data protection for data controllers and processors. These aspects are laid out legibly as follows:

- Section 1 General Obligations emphasises the responsibilities and compliance of data controllers and processors. This section including eight articles (Arts. 24-31) species the data controllers' duties to impose practical measures to ascertain the

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

GDPR compliance (Art. 24). It is their tasks not only to adopt data protection by design and by default but also to scrutinize the nature, scope, context and processing intentions (Art. 25). This section also stipulates the corresponding accountabilities of joint controllers in terms of ensuring data protection compliance (Art. 26). Moreover, it is mandatory for non-EU controllers or processors to have a representative within the EU take charge of transatlantic data exchange (Art. 27). Similarly, data processors are under the supervision of the controllers' instructions (Art. 28), and they jointly responsible for the security of the data (Art. 29). In addition, they are cooperatively in charge of archiving records of processing activities confidentially (Art. 30). Finally, this section states that it is compulsory for them to cooperate closely with their supervisory authorities regarding their performance on demand (Art. 31).

- Section 2 notifies the security of personal data, especially data protection and breach notifications; these regulations are laid down in Arts. 32-34. In particular, data controllers and processors are aware of a level of security which meets the requirement of the appropriate level of risk of data processing (Art. 32). In the event of personal data breaches, data controllers and supervisors have to report officially to the supervisory authority within 72 hours (Art. 33). Accordingly, it is necessary to establish communication of a personal data breach to the data subject in certain circumstances (Art. 34).
- Section 3 focuses on data protection impact assessment and prior consultation. In other words, this chapter specifies how to assess and consult on data protection risks in two articles (Arts. 35-36). Data protection impact assessments are necessary for high-risk processing, specified in Art. 35. In the same vein, prior consultation with the supervisory authority is required in case processing personal data might lead to a high risk in the lack of preventative measures implemented by the controllers to lower the potential risk (Art. 36).
- Section 4 particularises the roles and responsibilities of a data protection officer, which encompasses three articles (Arts. 37-39). Controllers and processors must appoint a Data Protection Officer (DPO) under certain conditions. The DPO shall be chosen on account of his/her professional experiences; that is, he/she shall have professional knowledge of data protection law, practical experience as well as the autonomous capacity to handle tasks effectively. The profiles of the data protection officer shall be available to the public and the supervisory (Art. 37). The DPO shall be involved properly and promptly in all matters related to the protection of personal data. Furthermore, he/she shall be under the control of secrecy or confidentiality regarding the lawful performance of his/her tasks. If the DPO is possibly designated to engage in other tasks and duties, he/she shall be aware of the fact that some tasks and responsibilities do not create a conflict of interest (Art. 38).

The DOP shall be under the supervision of the controllers or the processors and those who are involved in the processing of their obligations in accordance with the statutory

provisions. He/she shall regulate the lawfulness of the GDPR with other data privacy jurisdictions in respect of personal data protection. The detailed provisions are listed in Art. 39 thereof. The last section of Chapter 4 is Section 5, which encompasses codes of conduct and certification. The section establishes data protection standards in four articles (Arts. 40-43). In detail, codes of conduct shall be jointly drawn up to help demonstrate compliance with other legal normative documents for the purpose of the proper application of this regulation (Art. 40). The supervision of compliance with a code of conduct shall be monitored by a body with an appropriate level of expertise concerning the subject-matter of the code and is accredited for the commission by the competent supervisory authority (Art. 41).

Certification mechanisms shall be lawfully given by competent bodies that oversee the establishment of data protection certification mechanisms and of data protection seals and marks, which are directly provided by controllers or processors. The competent supervisory authority shall issue the certification mechanism to a controller or processor provided that this body has necessary documentation with all information and access to its processing activities under the provision of the certification procedure (Art. 42). The certification bodies shall take charge of issuing and renewing certification under legislative requirements. Those bodies must take full responsibility and duty to supervise all the procedures for the existence of data protection certification mechanisms (Art. 43).

Thirdly, Chapter 6 of the GDPR establishes the legal framework for establishing, operating, and powers of independent supervisory authorities in each member of the European countries. These authorities are crucial for protecting the free flow of personal data and the consistent application of the GDPR across the European Union (EU). They are endowed with investigative, corrective, and advisory powers and expected to operate with complete independence and adequate resources. Member States are responsible for their establishment, appointment of members, and for providing necessary resources, as well as reporting their activities to the Commission. This chapter comprises two sections. Section 1 focuses on the independent status of each Member State, while Section 2 delineates the competence, tasks, and powers of each Member State. Notably, Section 1 stipulates the independent status of each country in the EU, which covers four articles (Arts. 51-54).

Each Member State shall set up one or more independent public authorities to oversee the consistent application of this Regulation. To help the free flow of personal data within the Union, the State shall mandate one representative supervisory authority to officially take responsibility for coordinating with other authorities with regard to ensuring compliance with their competencies (Art. 51). The duties and liabilities of each supervisory authority shall be autonomous according to the Regulation. That is, the member of each supervisory authority shall carry out their duties independently without interference from outside influence as long as out of the scope and limitations of the Regulation. In other words, the independence of supervisory authorities is emphasised to ensure impartiality and objectivity in their duties. Each supervisory authority is endowed with the right to choose

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

and monitor their employees under the Regulation (Art. 52). The members of the supervisory authority are appointed under specific conditions to ensure their capability and integrity. These conditions may include a minimum term of four years and provisions for dismissal only under circumstances such as inability to perform duties or serious misconduct. Member States must notify the Commission of the laws adopted for the establishment of their supervisory authorities and any subsequent amendments (Art. 53).

Rules for the establishment of supervisory authority are clearly prescribed in the Regulation. Each Member State is subjected to the provisions detailed in the Regulation. Remarkably, each supervisory authority member and the staff shall comply with a duty of professional secrecy during and after their term of office. They are in charge of preserving confidential information throughout their lifetime (Art. 54).

Section 2 of Chapter 6 of GDPR deals with the competence, tasks, and powers of independent supervisory authorities. Specifically, supervisory authorities can perform tasks and exercise powers on their own Member State's territory. The details thereof are prescribed in Arts. 55-56. Typically, when more than one supervisory authority is established in a Member State, a mechanism is set to designate a lead supervisory authority to represent the others on the Board and ensure compliance with the consistency mechanism. The lead supervisory authority has specific responsibilities, including deciding whether to handle a case within three weeks of receiving a complaint.

The duties and competence of independent supervisory authorities are clearly designated in Articles 57-58 herein. These include monitoring and enforcing the GDPR, understanding risks, rules, safeguards, and rights related to data processing, and having governmental dominion over the business. Their powers are extensive, encompassing investigative, corrective authorisation, and advisory powers to ensure compliance with the GDPR.

Lastly, regarding activity reports, this Regulation is laid out in Art. 59 GDPR, in which supervisory authorities are required to produce annual activity reports detailing their activities related to GDPR compliance. These reports must be submitted in compliance with each Member State's law and made publicly available.

In reality, the GDPR not only identifies the role of data subjects but also recognises pseudonymised data, whose principles are enshrined in law, particularly in Art. 4(5) thereof. In a sense, "pseudonymisation" refers to the procedure of dealing with personal data process in which the personal data is anonymous to a specific data subject without the requirement of more information as long as the supplemented information is stored separately and under the control of technical and organisational means that personal data are not retrieved to an identified or identifiable natural person. In this regard, a natural person refers only to a living human being, so the GDPR does not cover and protect the decreased or the legal persons' data such as corporations.[32]

32 Finck (n 31).

According to the GDPR, there is a close tie between the data controllers and data processors in that the data controllers shall be in charge of the data processors if something wrong takes place, and this legal bond is laid down in detail at length in one chapter with 24 articles (Arts 24-42) therein. The GDPR also tries to keep data processors away from predictable principal-agent problems by regulating the controllers to solely take responsibility for being on behalf of the data processors, who must be competent and liable. To bear a chain of legal responsibilities, the controllers have the authority to supervise and be responsible for the processors for their disobedience. In other words, the controllers shall take charge of the processors' performance unless required by Union or Member State law (Art. 29 GDPR).

The GDPR is fundamentally built around seven key principles, which are considered the core of any legislative documentation. The seven principles of GDPR are laid out in Chapter 2, including seven articles (Arts. 5-11) designed to guide how personal data can be collected, processed, and managed by organizations or agencies with the consent of the data subjects. To make it more legitimate, suitable recitals are mentioned at the end of each article; thus, the GDPR can be seen as an overarching framework that is created to design its own broad objectives so that members of the European countries have to adjust their data protection rules lawfully to be in line with the GDPR.[33]

Overall, the GDPR is the most consequential regulatory development in information policy in the free flow of personal data protection policy in the age of the global digital economy. Yet, it brings privacy regulations into a complex and protective regulatory polity.

4 POTENTIAL CONFLICTS BETWEEN TWO LEGAL INSTRUMENTS IN PRACTICAL IMPLEMENTATION

In an era of data-driven decision-making, understanding the nuances of various data protection laws is crucial for businesses operating globally. The Decree represents the country's first comprehensive data protection law, aiming to safeguard the personal data of its citizens.[34] The introduction of the Decree has added a new dimension to this complex landscape, drawing comparisons to the well-established GDPR.[35] In general, GDPR and Vietnam's Decree have a broad scope, applying to entities within and outside their respective jurisdictions if they process relevant data subjects' personal data. The Decree applies to Vietnamese individuals and organisations, including those operating offshore and foreign entities operating in Vietnam or directly engaging in personal data

33 Manuel Klar, 'Binding Effects of the European General Data Protection Regulation (GDPR) on US Companies' (2020) 11(2) Hastings Science and Technology Law Journal 101; Pernot-Leplay (n 3); Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23(2) German Law Journal 226, doi:10.1017/glj.2022.18.

34 Decree no 13/2023/ND-CP (n 19).

35 GDPR (n 11).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

processing activities in Vietnam. GDPR similarly applies to any company that processes data on European residents, regardless of the company's location. While it shares commonalities with GDPR, notable differences impact how personal data is processed within Vietnam relating to the two regulatory frameworks due to differences in legal frameworks, enforcement mechanisms, and specific requirements. The following principal points shall be taken into careful consideration for the sake of preventing potential legal conflicts as follows:

a) Concerning scope and applicability, the Decree currently applies to a broad range of entities, including both domestic and foreign organisations or individuals processing personal data in Vietnam, as well as Vietnamese entities processing data outside of Vietnam, which is laid down in Art. 1. The GDPR, in contrast, applies to entities within the EU and those outside the EU that offer goods or services to, or monitor the behaviour of EU data subjects (Art. 3). This difference in scope denotes that businesses have to change their compliance strategies due to the geographic locations of their data subjects.
b) In terms of definitions and categories of data, the Decree, like the GDPR, sets out a detailed definition of personal data and clearly distinguishes between “basic” and “sensitive: personal data. According to the Decree (Art. 2), sensitive personal data constitute categories namely location data, creditworthiness, and financial data, which is considered more stringent and broader than the GDPR's definition of sensitive data (Art. 4) in that the GDPR does not categorise financial information into sensitive data.
c) Regarding consent and legal bases for processing, both the Decree and GDPR emphasise consent as a legal basis for processing personal data but differ significantly in their scope and flexibility of legal bases. The Decree does not recognise "legitimate interests" as a basis for processing, while the GDPR allows for a broader range of legal bases for processing, including legitimate interests, defined in Art. 7 therein. However, the Decree has more stringent consent rules and requires explicit consent for specific data processing activities, especially for sensitive personal data (Art. 11). This might lead to potential conflicts in case transatlantic personal data takes place.
d) As for data subject rights, both regulations grant data subjects a range of rights over their personal data, including the right to be informed, access, correct, delete, and restrict processing. The Decree also introduces the right to self-defense (Art. 9(11)), especially for sensitive personal data, which is not explicitly provided under the GDPR. In particular, the Decree introduces an absolute right to object to processing (Art. 12), as well as correction and deletion rights, and organisations must notify individuals of the consequences of withdrawing consent (Art. 13), which may differ from the GDPR's approach.
e) With regard to cross-border data transfers, the Decree has specific requirements for cross-border data transfers and introduces conditions such as obtaining consent for

the transfer of personal data (Art. 25); whereas, the GDPR has a different approach, allowing transfers based on adequacy decisions, appropriate safeguards, or specific derogations (Art. 44). Businesses must carefully take care of these requirements to ensure the lawful movement of data flows.

f) For data processing obligations, the Decree requires the establishment of a data protection department (Art. 29) and a data protection officer within organisations, with exemptions for certain enterprises until two years after their establishment. At the same time, the GDPR mandates the appointment of a data protection officer for specific organisations based on their core data processing activities but does not require the creation of a specific department (Art. 37). This difference highlights the varying emphasis on organisational accountability in data processing between the two regulations.

g) Concerning enforcement and sanctions, the Decree lacks a specific fine structure for violations, and the Department of Cybersecurity and Hi-tech Crime Prevention under the Ministry of Public Security (MPS) is entrusted with enforcement (Art. 30). In contrast, the GDPR provides a clear and prescriptive list of fines and sanctions for non-compliance (Arts. 77-84). This might bring about some difficulties in addressing the transborder flow of data.

h) With respect to prohibitions and purpose limitation, the Decree takes a more stringent stance by explicitly prohibiting the sale and purchase of personal data unless permitted by law (Art. 22). Although the GDPR imposes purpose limitation, it does not explicitly address the sale and purchase of personal data[36].

i) When considering the rights of the data subject, it is well noted that Art. 9 (11) stipulates the right to self-defence; that is, the data subject shall have the right to protect himself/herself in accordance with the Civil Code, other relevant laws and this Decree, or request competent agencies or organisations to implement methods of protection of civil rights prescribed in Art. 11 of the Civil Code.[37] This is a novel concept for Europeans and may deserve some additional explanation since the European legislators may consider whether to adopt this additional right, which is so far not contained in the GDPR.

Overall, Vietnam's Personal Data Protection Decree 2023 introduces a comprehensive data protection framework with several key differences from the GDPR. These differences include the legal bases for processing, data subject rights, cross-border data transfer requirements, enforcement mechanisms, and prohibitions on data sales. Since the Decree

36 Communication from the Commission to the European Parliament and the Council: First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')' of 25 July 2022 (COM(2022) 364 final) <https://commission.europa.eu/publications/first-report-application-and-functioning-data-protection-law-enforcement-directive-eu-2016680-led_en> accessed 10 March 2024.

37 Law of the Socialist Republic of Vietnam no 91/2015/QH13 of 24 November 2015 'Civil Code' <https://vietanlaw.com/the-law-no-91-2015-qh13/> accessed 10 March 2024.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

came into effect, these differences have become apparent, prompting the need for careful attention to ensure compliance with both Vietnamese and EU data protection laws. Further guidance from the Ministry of Public Security could offer clarification on the Decree's provisions and assist businesses in aligning their practices with the new requirements.

5 CONCLUSIONS

The GDPR and Vietnam's Decree play crucial roles in the protection of personal data. The GDPR's broad scope and stringent penalties have made it a global standard, while the Decree's comprehensive approach demonstrates Vietnam's commitment to data protection. Both regulations emphasise the importance of consent, data subject rights, and the safe handling of cross-border data transfers.

As data protection continues to gain prominence, the roles of these regulations in shaping data protection practices and ensuring compliance cannot be overstated. Organisations operating under the GDPR and Vietnam's Decree must carefully navigate the differences between the two regulations to avoid potential violations. While there are many similarities, the specific requirements around consent, data subject rights, breach notification, cross-border data transfers, and enforcement mechanisms can lead to conflicts. Businesses must understand both sets of regulations and ensure that their data protection practices are tailored to comply with each framework's unique requirements.

Breaching data protection regulations in the EU and Vietnam carries significant legal implications, including fines, penalties, and operational disruptions. While the GDPR is known for its hefty fines and broad scope, Vietnam's Decree introduces specific requirements and penalties that organisations must navigate carefully. It is crucial for entities operating in these jurisdictions to understand and comply with each regulation to avoid legal repercussions. In fact, the Decree adopts many of the GDPR's principles, such as the rights of data subjects, consent requirements, and the need for impact assessments; yet, it also includes provisions specific to the Vietnamese context, such as the absence of "legitimate interests" as a legal basis for processing and the unique enforcement mechanisms.

The implementation of Vietnam's Decree will have a profound impact on international companies operating in Vietnam. These companies must navigate the new requirements for consent, data processing, and cross-border data transfers, as well as adhere to data localisation mandates. The Decree aligns Vietnam's data protection standards with global norms, such as the GDPR, and introduces stringent measures to safeguard personal data. However, its effectiveness will depend on its enforcement mechanisms and the ability to impose meaningful sanctions for non-compliance. Given the Decree's alignment with global standards and its aim to protect the personal data of Vietnamese citizens, it is a strong candidate for becoming a personal data protection law. Nonetheless, to ensure its success, Vietnam may need to address the enforcement challenges and consider incorporating a more detailed sanctions regime to deter violations effectively.

REFERENCES

1. Comandè G and Schneider G, Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think' (2022) 23(4) German Law Journal 559, doi:10.1017/glj.2022.30.
2. Finck M, 'Hidden Personal Insights and Entangled in the Algorithmic Model: The Limits of the GDPR in the Personalisation Context' in U Kohl and J Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law* (CUP 2021) 95.
3. Gregorio G, 'The Transnational Dimension of Data Protection: Comparative Perspectives from Digital Constitutionalism' (2022) 1(2) The Italian Review of International and Comparative Law 335, doi:10.1163/27725650-01020006.
4. Hoofnagle CJ, Sloot B and Zuiderveen Borgesius F, 'The European Union General Data Protection Regulation: What it is and What it Means' (2019) 28(1) Information & Communications Technology Law 65, doi:10.1080/13600834.2019.1573501.
5. Hummel P, Braun M and Dabrock P, 'Own Data? Ethical Reflections on Data Ownership' (2020) 34 Philosophy & Technology 545, doi:10.1007/s13347-020-00404-9.
6. Klar M, 'Binding Effects of the European General Data Protection Regulation (GDPR) on US Companies' (2020) 11(2) Hastings Science and Technology Law Journal 101.
7. Long-Sutehall T, Sque M and Addington-Hall J, 'Secondary Analysis of Qualitative Data: A Valuable Method for Exploring Sensitive Issues with an Elusive Population' (2010) 16(4) Journal of Research in Nursing 335, doi:10.1177/1744987110381553.
8. Pernot-Leplay E, 'China's Approach on Data Privacy Law: A Third Way Between the US and the EU?' (2020) 8(1) Penn State Journal of Law & International Affairs 49.
9. Quinn P and Malgieri G, 'The Difficulty of Defining Sensitive Data - The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22(8) German Law Journal 1583, doi:10.1017/glj.2021.79.
10. Schwartz PM and Peifer KN, 'Transatlantic Data Privacy Law' (2017) 106(1) Georgetown Law Journal 115.
11. Seyyar MB and Geradts Z, 'Privacy impact assessment in large-scale digital forensic investigations' (2020) 33 Forensic Science International: Digital Investigation 200906, doi:10.1016/j.fsidi.2020.200906.
12. Tareck A, 'Legal Mechanisms for the Stimulation of the Digital Economy in Developing Countries' (2023) 6(Spec) Access to Justice in Eastern Europe 72, doi:10.33327/AJEE-18-6S002.
13. Taylor M, 'Data Protection and the Free Flow of Information' in Taylor M, *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality* (CUP 2023) 150, doi:10.1017/9781108784818.007.

14. Taylor M, 'Limits that Public International Law Poses on the European Union Safeguarding the Fundamental Right to Data Protection Extraterritorially' in Taylor M, *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality* (CUP 2023) 57, doi:10.1017/9781108784818.004.

15. Thouvenin F and Tamò-Larrieux A, 'Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market?' in Burri M (ed), *Big Data and Global Trade Law* (CUP 2021) 316, doi:10.1017/9781108919234.020.

16. Veale M and Zuiderveen Borgesius F, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23(2) German Law Journal 226, doi:10.1017/glj.2022.18.

17. Waerdt PJ, 'Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market' (2020) 38 Computer Law & Security Review 105436, doi:10.1016/j.clsr.2020.105436.

AUTHORS INFORMATION

Hoa Thanh Ha
Dr. Sc. (Law), Lecturer, **Faculty of International Law, Hanoi Law University, Hanoi, Vietnam**
hathanhhoa@hlu.edu.vn
https://orcid.org/0009-0000-5267-4865
Co-author, responsible for conceptualization, research methodology, data collection, writing – original draft, and supervising.

Tuan Van Vu*
Dr. Sc. (**English**), Lecturer, **Faculty of Legal Foreign Languages**, **Hanoi Law University, Hanoi, Vietnam**
tuanvv@hlu.edu.vn
https://orcid.org/0000-0002-3066-7338
Corresponding author, responsible for writing – review & editing.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that their opinion and views expressed in this manuscript are free of any impact of any organisations.

ABOUT THIS ARTICLE

Cite this article
Ha Thanh H and Vu Van T, 'Potential Conflicts in Personal Data Protection under Current Legislation in Vietnam Compared with European General Data Protection Regulation' (2024) 7(3) Access to Justice in Eastern Europe 505-26 <https://doi.org/10.33327/AJEE-18-7.3-a000304>

Submitted on 19 Mar 2024 / Revised 02 Apr 2024 / Approved 22 Apr 2024
Published ONLINE: 23 May 2024 / Last Published: 05 Aug 2024
DOI https://doi.org/10.33327/AJEE-18-7.3-a000304

Managing editor – Mag. Yuliia Hartman**. English Editor** – Julie Bold.

Keywords: *potential conflict, legislation, transatlantic data, privacy data, regulation.*

ACKNOWLEDGEMENT

This article was financially supported by Hanoi Law University.

RIGHTS AND PERMISSIONS

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Стаття-огляд

МОЖЛИВІ КОНФЛІКТИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗГІДНО З ЧИННИМ ЗАКОНОДАВСТВОМ В'ЄТНАМУ ПОРІВНЯНО З ЄВРОПЕЙСЬКИМ ЗАГАЛЬНИМ РЕГЛАМЕНТОМ ПРО ЗАХИСТ ДАНИХ

Хоа Тхань Ха та Туан Ван Ву*

АНОТАЦІЯ

Вступ. *Трансатлантична передача даних є критично важливим компонентом глобальної цифрової економіки, що сприяє торгівлі та комунікації між країнами в усьому світі. Однак ці передачі пов'язані з правовими та регулятивними проблемами, зокрема щодо захисту персональних даних через відсутність комплексного глобального закону про конфіденційність.*

Методи. *У цьому порівняльно-описовому дослідженні використовуються вторинні ресурси за допомогою порівняння та протиставлення принципів європейського Загального регламенту про захист даних і нового Указу про захист персональних даних у В'єтнамі, щоб забезпечити глибоке розуміння відмінностей між ними.*

Результати та висновки. *Незважаючи на те, що Указ використовує багато принципів європейського Загального регламенту про захист даних, а саме права суб'єктів даних, вимоги щодо згоди та необхідність оцінки впливу, він містить положення, специфічні для в'єтнамського контексту, такі як унікальні механізми забезпечення та відсутність «законних інтересів» як правової основи для обробки. Незважаючи на багато спільного, конкретні вимоги щодо згоди, прав суб'єктів даних, повідомлення про порушення, екстериторіальної передачі даних і механізмів, що забезпечуватимуть виконання, можуть призвести до конфліктів між цими законодавчими документами. Указ, який міг би стати ефективнішим, має спиратися на механізми його виконання та можливість накладати значні санкції за невиконання; таким чином, він повинен містити більш детальний режим санкцій для ефективного стримування порушень.*

Ключові слова: *можливий конфлікт, законодавство, трансатлантичні дані, конфіденційність даних, регулювання.*