# Personal Data Protection in the Data Economy: A Study of European Union Law and Lessons for Vietnam

**Nguyen Ngoc Sang -** Lecturer, Faculty of Law, Binh Duong University, Ho Chi Minh City, Vietnam[1]

## ABSTRACT

*In the context of the growing data economy, personal data serves both as a driver of economic growth and as a potential source of human rights violations. Although Vietnam has gradually established a legal foundation for personal data protection through constitutional and statutory provisions, significant legal gaps remain, particularly regarding the comprehensive recognition and effective enforcement of data subjects' rights, as well as the lack of coherence among legal mechanisms designed to ensure individuals' ability to proactively control, manage, and protect their personal data in practice. Furthermore, Vietnam has yet to establish a supervisory authority with the degree of institutional independence required under the European Union's data protection model, while the practical effectiveness and deterrent impact of its newly introduced enforcement mechanisms remain subject to further assessment and verification. Against this background, this article examines the European Union's legal framework and compares it with Vietnamese law, thereby proposing legal reforms aimed at adopting a data subject-centered approach, strengthening the effectiveness of enforcement mechanisms, and ensuring an appropriate balance between the development of the digital economy and the protection of individuals' rights to personal data.*

***Keywords:*** *Personal Data, Data Economy, Digital Economy, Human Rights.*

## 1. INTRODUCTION

The data economy has become an increasingly important component of contemporary socioeconomic development, with digital data serving as a strategic resource for innovation, productivity enhancement, and economic competitiveness. The growing capacity to collect, process, and analyze large volumes of data has enabled the development of new products, services, and data-driven business models.[2] According to the European Commission (2020, p. 6), the EU's data economy was valued at approximately EUR 325 billion in 2019, accounting for 2.6% of its GDP. Nevertheless, the economic benefits derived from personal data processing are accompanied by significant risks to fundamental rights, particularly the rights to privacy, freedom of expression, and non-discrimination. Through the aggregation and analysis of digital traces, organizations can construct detailed profiles of individuals, potentially enabling continuous monitoring and the assessment of their characteristics, preferences, and behavior.[3] Furthermore, empirical research demonstrates that psychologically targeted communication can influence individual behavior, while algorithmic profiling may generate discriminatory outcomes that are difficult to identify and challenge.[4] Recent experimental evidence also indicates that concerns about data surveillance may discourage individuals from engaging in otherwise lawful online communication. These developments highlight the potential for personal data processing to undermine individual

[1] Nguyen Ngoc Sang, LL.M., Lecturer, Faculty of Law, Binh Duong University, Ho Chi Minh City, Vietnam; Ph.D. candidate. Email: nn.sang@bdu.edu.vn; ORCID: https://orcid.org/0009-0007-4035-1285.

[2] Mujahid Mohiuddin Babu et al., *Exploring Big Data-Driven Innovation in the Manufacturing Sector: Evidence from UK Firms*, 333 Annals of Operations Research 689 (2024), https://doi.org/10.1007/s10479-021-04077-1.

[3] Andrea Armstrong et al., *Everyday Digital Traces*, 10 Big Data & Society 20539517231213827 (2023), https://doi.org/10.1177/20539517231213827.

[4] S. C. Matz et al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 114 Proceedings of the National Academy of Sciences 12714 (2017), https://doi.org/10.1073/pnas.1710966114.

autonomy, cause reputational or socioeconomic harm, and restrict the effective exercise of fundamental rights, thereby reinforcing the need for transparent, accountable, and rights-based data governance.

Balancing the development of the digital economy with the protection of fundamental human rights requires a legal framework that promotes responsible data use while safeguarding privacy and individual autonomy.[5] The European Union exemplifies a rights-based approach, with Articles 7 and 8 of the Charter of Fundamental Rights recognizing the rights to privacy and personal data protection, further implemented through the General Data Protection Regulation (GDPR). In Vietnam, Article 21 of the 2013 Constitution provides a constitutional foundation for privacy protection, subsequently reinforced by the Law on Personal Data Protection No. 91/2025/QH15 and Decree No. 356/2025/ND-CP. Nevertheless, the effectiveness of this evolving legal framework depends on consistent enforcement, institutional accountability, and effective mechanisms for protecting individual rights in the digital economy.[6]

## 2. THEORETICAL FOUNDATIONS OF PERSONAL DATA PROTECTION IN THE DATA ECONOMY

### 2.1. Overview of Personal Data Protection in the data economy

The protection of personal data is rooted in the fundamental human right to privacy, which has been progressively recognized and developed through international and regional human rights instruments. Article 12 of the Universal Declaration of Human Rights (1948) establishes an international human rights standard protecting individuals against arbitrary interference with their privacy, family, home, and correspondence. This protection is further reflected in Article 17 of the International Covenant on Civil and Political Rights (1966), which establishes binding treaty obligations for States Parties. At the regional level, Article 8 of the European Convention on Human Rights (1950) guarantees the right to respect for private and family life, home, and correspondence, while permitting interference by public authorities only under legally prescribed conditions consistent with the requirements of necessity in a democratic society. These legal instruments provide a foundation for understanding privacy protection not merely as a limitation on arbitrary state interference but also as a source of positive obligations requiring States to establish effective legal safeguards against infringements by private actors.[7] Accordingly, personal data protection has evolved into an increasingly significant dimension of human rights protection in the digital environment.[8]

The data economy is characterized by the extensive collection, processing, and utilization of data to generate economic value through digital platforms, algorithmic systems, and artificial intelligence. Although these developments facilitate innovation and the emergence of new business models, they also create significant challenges concerning individuals' ability to exercise meaningful control over their personal information. These challenges are particularly evident in digital services that rely on the commercial exploitation of user data rather than direct monetary payments. Custers and Malgieri (2022) argue that treating personal data as an ordinary commercial commodity is fundamentally problematic under EU data protection law because the rights of data subjects cannot simply be alienated through market transactions.[9] In this context, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union recognize the right to respect for private life and the right to the protection of personal data as distinct but closely related fundamental rights. These rights are further

[5] Inge Graef et al., *Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice*, 2 Digital Society 19 (2023), https://doi.org/10.1007/s44206-023-00045-3.
[6] Ngoc Tuan Tran, *Human-Centric Approaches to Digital Privacy: Insights from the Europe with Implications for Vietnam*, 13 Social Sciences & Humanities Open 102926 (2026), https://doi.org/10.1016/j.ssaho.2026.102926.
[7] Yuliia Kovalenko, *The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights*, 16 Masaryk University Journal of Law and Technology 37 (2022), https://doi.org/10.5817/MUJLT2022-1-2.
[8] Vo Trung Hau, *Human Rights and Control of Personal Data in the Digital Economy: EU Legal Case Studies and Recommendations for Vietnam*, 14 Ius Humani. Law Journal 137 (2025), https://doi.org/10.31207/ih.v14i1.409.
[9] Bart Custers & Gianclaudio Malgieri, *Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data*, 45 Computer Law & Security Review 105683 (2022), https://doi.org/10.1016/j.clsr.2022.105683.

operationalized through the General Data Protection Regulation, which establishes principles of lawful processing, transparency, accountability, and data subject control. In particular, Article 7(3) of the GDPR recognizes the right to withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing undertaken before withdrawal. This mechanism constitutes an important safeguard of informational autonomy while demonstrating the legal limitations imposed on the commercialization of personal data.

In the context of increasingly sophisticated digital technologies, personal data protection must also be examined in relation to other fundamental rights, particularly freedom of expression, access to information, and non-discrimination. Algorithmic personalization may, under certain conditions, contribute to the formation of information filter bubbles by reducing users' exposure to diverse viewpoints. However, empirical research indicates that such effects are not inevitable and depend significantly on the design and operation of recommendation systems. Similarly, artificial intelligence systems may reproduce or amplify existing social biases, potentially resulting in discriminatory outcomes in recruitment, credit assessment, and other automated decision-making processes.[10] These developments demonstrate that effective personal data protection cannot rely exclusively on individual consent but also requires transparency, accountability, non-discrimination, and appropriate safeguards against the adverse effects of algorithmic decision-making. In Vietnam, Article 21 of the 2013 Constitution recognizes the inviolability of private life, personal secrets, and family secrets, establishing a constitutional foundation for the protection of personal information. This foundation has been further developed through the Law on Personal Data Protection No. 91/2025/QH15, effective from January 1, 2026, and its implementing regulations. Nevertheless, the effectiveness of this legal framework depends not only on the formal recognition of data subject rights but also on the establishment and implementation of mechanisms capable of ensuring compliance, accountability, and effective remedies in the rapidly evolving digital economy.

### 2.2. European Union legal framework for personal data protection in the data economy

Within the European Union, personal data protection is recognized as a fundamental right with constitutional significance, reflecting a rights-based approach to data governance in the digital economy. Article 8 of the Charter of Fundamental Rights of the European Union expressly guarantees the right to the protection of personal data, while Article 16 of the Treaty on the Functioning of the European Union provides an additional constitutional basis for the establishment of data protection legislation. These guarantees are operationalized through Regulation (EU) 2016/679, commonly known as the General Data Protection Regulation (GDPR), which has applied since May 25, 2018. By establishing harmonized principles, enforceable individual rights, and corresponding obligations for data controllers and processors, the GDPR seeks to strengthen fundamental rights protection while facilitating the lawful movement of personal data within the EU Digital Single Market.[11]

A central component of the GDPR is the comprehensive system of rights granted to data subjects. Articles 12–15 establish requirements concerning transparent information and the right of access, enabling individuals to obtain information about the collection and processing of their personal data. Article 16 provides the right to rectification, while Article 17 establishes the right to erasure, commonly referred to as the "right to be forgotten." Nevertheless, the right to erasure is not absolute and must be exercised in accordance with the conditions and exceptions prescribed by the GDPR, including those relating to freedom of expression and information, legal obligations, and certain public interests. As Kohl (2023) demonstrates, the right to be forgotten illustrates the complex relationship between individual control over personal information and competing interests in maintaining access to information.[12] Furthermore, Articles 18, 20, and 21 recognize the rights to restriction of processing, data portability, and objection to processing, respectively. In particular, data portability seeks to strengthen individual

[10] Ana Cristina Bicharra Garcia et al., *Algorithmic Discrimination in the Credit Domain: What Do We Know About It?*, 39 AI & Society 2059 (2024), https://doi.org/10.1007/s00146-023-01676-3.
[11] Damian Eke & Bernd Stahl, *Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies*, 3 Digital Society 11 (2024), https://doi.org/10.1007/s44206-024-00101-6.
[12] Uta Kohl, *The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy*, 72 International and Comparative Law Quarterly 737 (2023), https://doi.org/10.1017/S0020589323000258.

control over personal data while facilitating interoperability and competition between digital service providers, although its application remains subject to specific legal conditions.[13]

The GDPR also establishes safeguards against certain forms of automated decision-making, including profiling. Under Article 22, individuals have the right not to be subject to decisions based solely on automated processing where such decisions produce legal effects concerning them or similarly significantly affect them, subject to the exceptions and safeguards prescribed by the Regulation. This protection is particularly relevant to data-driven decisions affecting employment, financial services, and other important aspects of individual life. Although earlier scholarship identified uncertainties concerning the scope of individuals' rights to obtain explanations of automated decisions,[14] subsequent jurisprudence has further clarified the applicable safeguards. In Case C-634/21,[15] the Court of Justice of the European Union addressed the application of Article 22 to automated credit scoring. Subsequently, in Case C-203/22,[16] the Court clarified that Article 15(1)(h) may require data controllers to provide meaningful explanations of the procedures and principles actually applied in automated decision-making falling within the scope of Article 22. In addition, Article 7(3) GDPR allows data subjects to withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing undertaken before its withdrawal. Together, these provisions establish safeguards aimed at protecting individual autonomy and accountability in data-driven decision-making.

Alongside individual rights, the GDPR imposes extensive obligations on organizations involved in personal data processing. These include compliance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability under Article 5; the implementation of appropriate technical and organizational security measures under Article 32; personal data breach notification requirements under Articles 33 and 34; and data protection impact assessments for processing operations likely to result in high risks to individuals' rights and freedoms under Article 35. Moreover, Article 3 establishes a territorial scope that extends, under specified conditions, to controllers and processors outside the Union where processing activities relate to the offering of goods or services to individuals in the Union or the monitoring of their behavior within the Union. This framework reflects the EU's approach to protecting personal data in circumstances involving transnational digital services and cross-border processing, while also raising questions concerning jurisdictional conflicts and the practical enforcement of data protection obligations.[17]

The effectiveness of the GDPR is further supported by independent supervisory authorities vested with investigative and corrective powers, together with cooperation and consistency mechanisms involving the European Data Protection Board. Under Article 83, certain serious infringements may result in administrative fines of up to EUR 20 million or 4% of an undertaking's total worldwide annual turnover in the preceding financial year, whichever is higher. These enforcement arrangements are intended to ensure that personal data protection operates not merely as a declaration of fundamental rights but as a system of legally enforceable obligations. Nevertheless, the effectiveness of the regulatory framework depends on consistent supervision, cross-border regulatory cooperation, and the practical accessibility of remedies for affected individuals.

Beyond the GDPR, the EU has developed complementary legislation addressing specific dimensions of the digital economy. Directive 2002/58/EC, commonly known as the ePrivacy Directive, establishes sector-specific rules governing the confidentiality of electronic communications, including the processing of certain traffic and location data and access to information stored in users' terminal equipment. The proposed ePrivacy Regulation, intended to replace this Directive, was withdrawn in 2025 and therefore does not form part of the applicable EU regulatory framework. At the same time, Regulation (EU) 2022/868, known as the Data Governance Act, establishes

[13] Paul De Hert et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 Computer Law & Security Review 193 (2018), https://doi.org/10.1016/j.clsr.2017.10.003.
[14] Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 International Data Privacy Law 76 (2017), https://doi.org/10.1093/idpl/ipx005.
[15] Case C-634/21, *OQ v. Land Hessen* (SCHUFA Holding AG intervening), ECLI:EU:C:2023:957 (Dec. 7, 2023).
[16] Case C-203/22, *CK v. Magistrat der Stadt Wien* (Dun & Bradstreet Austria GmbH intervening), ECLI:EU:C:2025:117 (Feb. 27, 2025).
[17] Federico Fabbrini & Edoardo Celeste, *The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders*, 21 German Law Journal 55 (2020), https://doi.org/10.1017/glj.2020.14.

mechanisms to facilitate trustworthy data sharing, including rules concerning data intermediation services and data altruism. Regulation (EU) 2023/2854, known as the Data Act, which has applied principally since September 12, 2025, introduces harmonized rules on fair access to and use of data, particularly data generated through connected products and related services. The Data Act grants users specified rights concerning access to and sharing of such data, while establishing additional rules on business-to-business data sharing, certain public-sector access requests, and switching between data processing services. Importantly, these mechanisms apply within the broader EU legal framework and do not displace the requirements of the GDPR when personal data is involved.[18]

Taken together, these legal instruments demonstrate the development of an integrated European approach to data governance, in which the protection of fundamental rights coexists with objectives concerning innovation, competition, and the economic utilization of data. Rather than replacing personal data protection with unrestricted data commercialization, the EU has developed complementary regulatory frameworks intended to facilitate data access and sharing under specified legal conditions while preserving fundamental rights safeguards. This approach reflects an ongoing effort to reconcile data protection with the free movement and economic utilization of data, although its effectiveness remains dependent on the implementation and further development of the European data strategy.[19]

### 2.3. Vietnamese legal framework for Personal Data Protection in the data economy

In Vietnam, the legal protection of personal data is grounded in constitutional guarantees concerning privacy and the protection of personal information. Article 21 of the 2013 Constitution recognizes the inviolability of private life, personal secrets, and family secrets, while Article 38 of the 2015 Civil Code further establishes legal safeguards for these interests. Building upon these constitutional and civil law foundations, Vietnam has progressively developed a specialized legal framework for personal data protection, particularly through the Law on Personal Data Protection No. 91/2025/QH15, which entered into force on January 1, 2026, and its implementing Decree No. 356/2025/ND-CP. Article 2 of the Law defines personal data as digital data or information in other forms that identifies or enables the identification of a specific individual, distinguishing between basic and sensitive personal data. The Law also provides that personal data which has undergone de-identification is no longer classified as personal data. Nevertheless, the effectiveness of this distinction depends on whether de-identification genuinely prevents the identification of individuals, particularly given empirical evidence demonstrating the possibility of re-identifying individuals from seemingly anonymized datasets.[20] These developments indicate Vietnam's transition toward a more comprehensive statutory framework for personal data protection in the digital economy.

A significant advancement of the 2025 Law is the express recognition of data subjects' rights and the corresponding responsibilities of entities processing personal data. Article 4 recognizes rights concerning information about processing activities, consent and withdrawal of consent, access to and rectification of personal data, requests for erasure or restriction of processing, objections to processing, complaints, legal proceedings, and compensation for damage. These rights are further specified through provisions governing consent, withdrawal of consent, rectification, and erasure under Articles 9, 10, 13, and 14. The Law also establishes principles concerning purpose limitation, accuracy, appropriate retention periods, and organizational and technical protection measures. Nevertheless, these rights are subject to statutory conditions and exceptions, and their effective exercise depends on the accessibility of legal procedures and the responsiveness of data controllers. Compared with the GDPR, the Vietnamese framework has not yet established a general right to data portability equivalent in scope and structure to Article 20 GDPR, notwithstanding its recognition of the right to request the provision of personal data. Consequently, the central issue is no longer merely the formal recognition of data

[18] Federico Casolari et al., *The EU Data Act in Context: A Legal Assessment*, 31 International Journal of Law and Information Technology 399 (2023), https://doi.org/10.1093/ijlit/eaae005.
[19] Pieter Wolters, *The Influence of the Data Act on the Shifting Balance Between Data Protection and the Free Movement of Data*, 15 European Journal of Law and Technology, no. 1, 2024, https://ejlt.org/index.php/ejlt/article/view/991 (last visited Nov. 16, 2026).
[20] Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 Nature Communications 3069 (2019), https://doi.org/10.1038/s41467-019-10933-3.

subjects' rights but also the effectiveness, enforceability, and practical accessibility of the mechanisms through which those rights may be exercised.

The relationship between personal data protection and national cybersecurity is further regulated by the Law on Cybersecurity No. 116/2025/QH15, which entered into force on July 1, 2026. Clause 3 of Article 4 establishes the principle of combining cybersecurity protection with socioeconomic development, the safeguarding of human rights and citizens' rights, and the protection of personal data. More specifically, Article 25(3) of the 2025 Cybersecurity Law imposes data-protection and domestic-storage obligations on the covered service providers, while Article 26 establishes broader data-security requirements, including periodic risk assessment and the assessment of cross-border data transfers. These provisions demonstrate the integration of cybersecurity and data governance into Vietnam's digital regulatory framework. Nevertheless, data localization and cross-border transfer requirements also raise questions concerning legal certainty, proportionality, regulatory compliance, and the free flow of data in the digital economy. Do and Selvadurai (2026) observe that although the consolidation of Vietnam's cybersecurity legislation strengthens regulatory coherence and state capacity, broadly formulated obligations and administrative discretion may create challenges for legal predictability and the protection of individual rights.[21] Similarly, Duc Anh Nguyen (2026) emphasizes the continuing tension between data sovereignty, domestic regulatory autonomy, and international commitments concerning cross-border digital trade.[22]

The enforcement framework for personal data protection has also undergone significant development. Article 33(1)(a) identifies the specialized personal-data-protection body within the Ministry of Public Security as a component of Vietnam's personal-data-protection force, while Article 36 assigns the Ministry of Public Security the principal state-management role in this field. Articles 20 and 21 establish impact assessment obligations concerning cross-border personal data transfers and personal data processing, subject to specified exemptions, while Article 37 provides obligations for data controllers and processors. Furthermore, Article 8 establishes differentiated maximum penalties. For the unlawful purchase or sale of personal data, the maximum administrative fine may be calculated at ten times the proceeds obtained from the violation, subject to the statutory fallback rule. For certain cross-border personal-data-transfer violations committed by organizations, the maximum fine may reach five per cent of the organization's revenue in the preceding year. These provisions represent a substantial strengthening of Vietnam's regulatory framework. Nevertheless, unlike the independent supervisory authorities established under Articles 51 and 52 GDPR, Vietnam's specialized data protection authority remains institutionally situated within the executive administration. Accordingly, important questions remain concerning the independence of regulatory oversight, the proportionality and consistency of enforcement, and the availability of effective remedies for individuals affected by unlawful data processing.

The growing application of big data analytics, algorithmic profiling, and artificial intelligence introduces further challenges to the protection of privacy and other fundamental rights. In commercial digital environments, behavioral advertising and personalized content delivery may involve extensive monitoring and analysis of users' online activities, potentially influencing individual choices and communication practices. Empirical research indicates that advertising-related data surveillance may produce chilling effects, as individuals adjust their online behavior in response to perceived monitoring.[23] Similarly, political microtargeting raises concerns regarding informational autonomy and the potential manipulation of opinions, although the actual effects of such techniques require careful empirical assessment rather than presumptions of universal effectiveness.[24] In response to

[21] Thi Ha Do & Niloufer Selvadurai, *Data Sovereignty and the Digital Economy: Analysing the Effectiveness of Viet Nam's Cyber Security and Cybercrime Laws*, Asian Journal of Law and Society 1 (2026) (published online July 14, 2026), https://doi.org/10.1017/als.2026.10056.

[22] Duc Anh Nguyen, *Between Digital Trade Commitments and Sovereignty: Asian Developing Members' Approaches to the CPTPP's Cross-Border Data Transfers*, Asian Journal of Law and Society 1 (2026) (published online Sept. 24, 2026), https://doi.org/10.1017/als.2026.10057.

[23] Joanna Strycharz & Claire M. Segijn, *Ethical Side-Effect of Dataveillance in Advertising: Impact of Data Collection, Trust, Privacy Concerns and Regulatory Differences on Chilling Effects*, 173 Journal of Business Research 114490 (2024), https://doi.org/10.1016/j.jbusres.2023.114490.

[24] Peter Aagaard & Selma Marthedal, *Political Microtargeting: Towards a Pragmatic Approach*, 12 Internet Policy Review, no. 1 (2023), https://doi.org/10.14763/2023.1.1690.

emerging technological risks, Vietnam has introduced more specific safeguards through the Law on Artificial Intelligence No. 134/2025/QH15, effective from March 1, 2026. This legislation establishes human-centered principles, requirements concerning fairness, transparency, human oversight, and risk-based management of AI systems. Furthermore, Article 10 of Decree No. 356/2025/ND-CP addresses personal data protection in AI systems, including requirements concerning notification of automated processing, explanations of algorithmic principles and their effects on data subjects, and opportunities to decline participation. These measures indicate an emerging regulatory approach extending beyond traditional data security toward the protection of individual rights in automated data processing.

Despite these legislative developments, the balance between personal data protection, national security, and socioeconomic development remains an important issue for further legal evaluation. Article 19 permits processing without the data subject's consent only in specified statutory circumstances. These include urgent situations involving the protection of life, health, dignity, or lawful rights and interests, and the necessary protection of legitimate rights or interests against infringement, as well as emergencies, national-security threats, crime prevention, legally prescribed state activities, the performance of agreements with the data subject, and other cases provided by law. Comparative research on consent exceptions also highlights the importance of defining lawful purposes and applying safeguards proportionate to the risks involved.[25] Furthermore, the institutional structure of data protection supervision, the scope of impact assessment exemptions, and the practical implementation of individual rights raise questions regarding whether existing protections are sufficiently effective in data-intensive environments. Therefore, the principal challenge for Vietnam is not the absence of a statutory personal data protection framework, but the need to ensure that its implementation provides meaningful individual control, transparent and accountable processing practices, effective regulatory supervision, and accessible remedies. Strengthening these dimensions would contribute to a more coherent rights-based data governance framework capable of protecting fundamental rights while supporting the sustainable development of Vietnam's digital economy.

## 3. COMPARATIVE ANALYSIS OF THE EUROPEAN UNION AND VIETNAMESE LEGAL FRAMEWORKS FOR PERSONAL DATA PROTECTION IN THE DATA ECONOMY

Firstly, regarding the scope and objectives of regulation, the European Union recognizes personal data protection as a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union. This constitutional foundation is further developed through the General Data Protection Regulation, which establishes a rights-based framework designed to protect individual autonomy while facilitating the lawful processing and movement of personal data within the digital economy. As Seubert and Becker (2021) emphasize, the protection of privacy and personal data has significance beyond individual interests, contributing to the preservation of fundamental rights and democratic values in the digital environment.[26] In Vietnam, Article 21 of the 2013 Constitution similarly establishes constitutional safeguards for private life and personal information, while the Law on Personal Data Protection No. 91/2025/QH15 provides more specific statutory protections. However, Vietnam's regulatory framework also incorporates objectives relating to national security, public order, and data sovereignty. The study by Do Thi Ha and Selvadurai suggests that these issues remain significant in the development and refinement of Vietnam's legal framework governing cybersecurity and data governance.[27] Accordingly, the principal distinction does not lie in whether individual rights are recognized, but rather in the constitutional status of personal data protection, the relative emphasis placed on different regulatory objectives, and the institutional mechanisms established to safeguard those rights.

[25] Anh Thu Nguyen, *Processing of Personal Data Without Consent for the Protection of Life and Health in Vietnam: A Comparison with European Union Law*, 3 Social Sciences in Brief 1 (2026), https://doi.org/10.47909/ssb.27.
[26] Sandra Seubert & Carlos Becker, *The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection*, 22 German Law Journal 31 (2021), https://doi.org/10.1017/glj.2020.101.
[27] Do & Selvadurai, *supra* note 21.

Secondly, regarding enforcement mechanisms and sanctions, the GDPR establishes a regulatory framework supported by independent supervisory authorities, with Articles 51 and 52 requiring Member States to ensure their institutional and functional independence. These authorities possess investigative and corrective powers, including the authority to impose administrative fines under Article 83. For certain serious infringements, the maximum fine may reach EUR 20 million or 4% of an undertaking's total worldwide annual turnover in the preceding financial year, whichever is higher. In Vietnam, the enforcement of personal data protection legislation is primarily administered through competent state authorities, with the specialized personal data protection authority established within the Ministry of Public Security under Article 33 of the 2025 Law. Nevertheless, Vietnamese legislation has introduced substantial sanctions, including maximum administrative fines calculated by reference to unlawful proceeds from personal data trading and, for certain violations concerning cross-border data transfers, the organization's revenue in the preceding year. Therefore, the difference between the two systems cannot be reduced to the severity of financial penalties. Instead, it primarily concerns the institutional independence of supervisory authorities, the organization of regulatory oversight, and the mechanisms through which enforcement decisions are reviewed and individual rights are protected. In this respect, the proportionality and practical effectiveness of regulatory enforcement remain important considerations for Vietnam's developing data protection framework.

Thirdly, regarding cross-border personal data transfers, the European Union and Vietnam pursue the common objective of ensuring continued personal data protection while facilitating lawful data flows, but adopt different regulatory approaches. Under Chapter V of the GDPR, transfers to third countries or international organizations may be based on adequacy decisions under Article 45, appropriate safeguards under Article 46, or specific derogations under Article 49, subject to the applicable legal conditions. By contrast, Vietnam’s framework, particularly Article 20 of the Law on Personal Data Protection No. 91/2025/QH15 and Articles 17–18 of Decree No. 356/2025/ND-CP, places relatively greater emphasis on cross-border transfer impact assessments and administrative supervision. Organizations and individuals subject to these requirements must prepare and submit the relevant impact assessment dossiers within the prescribed period, unless a statutory exemption applies, while competent state authorities retain the power to intervene in circumstances involving national defense or security, subject to the conditions established by law. As Hoang Le Ngoc Tien Dat and Chu Thi Thanh An (2024)[28] highlight, effective regulation of cross-border data flows requires clearly defined legal obligations and appropriate safeguards. Although both systems seek to balance personal data protection with the lawful movement of data, their differences lie primarily in the mechanisms through which transfer-related risks are assessed and regulatory responsibilities are allocated. The central comparative question is therefore not merely whether cross-border transfers are permitted, but how each framework ensures legal predictability, accountability, and effective protection after personal data have been transferred. This distinction provides a basis for evaluating the strengths and limitations of Vietnam’s regulatory approach in light of the European Union’s experience.

Fourthly, regarding legislative language and regulatory techniques, the GDPR employs broadly applicable principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability, which are designed to operate across different forms of technological processing. This approach provides a degree of technological neutrality and regulatory flexibility, allowing legal obligations to remain applicable despite changes in digital technologies. Jakobi et al. (2020) observe that the principle-based and risk-oriented structure of the GDPR may facilitate innovation while also creating challenges concerning legal certainty and regulatory interpretation.[29] Vietnamese legislation similarly adopts relatively broad definitions of personal data and establishes general principles governing data processing. Consequently, technological neutrality should not be regarded as an exclusive characteristic of EU law. Rather, the comparative challenge for Vietnam lies in developing a coherent combination of technology-neutral legal principles, sufficiently precise regulatory obligations, proportionate risk-based safeguards, and effective mechanisms for interpreting and enforcing the law.

[28] Hoang Le Ngoc Tien Dat & Chu Thi Thanh An, *The Regulation of Data Transmission in the Digital Era: From the European Union’s Perspective and Implications for Vietnam*, 11 Vietnamese Journal of Legal Sciences 1 (2024), https://doi.org/10.2478/vjls-2024-0007.

[29] Timo Jakobi et al., *The Role of IS in the Conflicting Interests Regarding GDPR*, 62 Business & Information Systems Engineering 261 (2020), https://doi.org/10.1007/s12599-020-00633-4.

Such an approach would enhance legal certainty while preserving the flexibility required to respond to technological developments and emerging risks in the data economy.

Overall, the comparison demonstrates that both the European Union and Vietnam seek to reconcile personal data protection with the development of the digital economy, although their legal frameworks differ in constitutional foundations, supervisory structures, cross-border transfer mechanisms, and regulatory implementation. The European experience provides useful comparative insights into independent oversight, enforceable data subject rights, and risk-based regulatory design. However, the adaptation of these mechanisms to Vietnam requires consideration of its constitutional framework, institutional structure, and socioeconomic conditions. Accordingly, strengthening personal data protection should involve not merely increasing regulatory obligations or sanctions, but also improving institutional accountability, legal certainty, the effective exercise of data subjects' rights, and the proportionality of regulatory measures in the digital economy.

## 4. LESSONS LEARNED AND RECOMMENDATIONS FOR VIETNAM

Firstly, refining the legal framework and strengthening data subject rights. In light of Vietnam's recent legislative developments, particular attention should be given to ensuring the consistent and effective implementation of the Law on Personal Data Protection 2025 and its implementing regulations. Drawing on the experience of the GDPR, Vietnam should further clarify the interpretation and application of technology-neutral legal concepts, particularly the criteria for identifying personal data and distinguishing effectively de-identified information from data that remains reasonably capable of identifying individuals. Such clarification should take into account technological developments and the potential combination of different datasets, thereby preventing regulatory gaps without unnecessarily expanding the scope of legal obligations. Furthermore, efforts should focus on improving the practical enforceability of existing data subject rights and examining the feasibility of introducing a more comprehensive right to data portability. These measures would strengthen individual control over personal data while promoting legal certainty and adaptability in the digital economy.

Secondly, enhancing institutional oversight and enforcement effectiveness. The experience of the European Union demonstrates the importance of effective and sufficiently independent regulatory oversight in ensuring compliance with personal data protection legislation. Although Vietnam has established a specialized personal data protection authority within the Ministry of Public Security, further improvements should focus on strengthening its professional capacity, operational transparency, and the objectivity of supervisory activities. In particular, consideration should be given to developing clearer procedures for handling complaints, conducting inspections, reviewing enforcement decisions, and ensuring coordination among competent authorities. Regarding sanctions, Vietnam's current legislation already provides substantial administrative penalties, including mechanisms based on unlawful proceeds and organizational revenue for certain violations. Therefore, reform priorities should focus not merely on increasing financial penalties but on ensuring their proportionality, consistent application, and effective enforcement. These measures would contribute to strengthening institutional accountability and ensuring that the protection of personal data is effectively implemented in practice.

Thirdly, strengthening rights-based data governance and safeguards against emerging technological risks. Personal data protection in the digital economy requires more than technical data security measures; it also demands effective mechanisms to safeguard individual autonomy, dignity, equality, and other fundamental rights. Accordingly, Vietnam should further strengthen the practical implementation of transparency requirements, accountability mechanisms, and individual rights in data-intensive processing activities, particularly those involving automated decision-making and artificial intelligence. Greater emphasis should be placed on ensuring meaningful explanations of consequential automated processing, appropriate human oversight, and safeguards against discriminatory outcomes, in accordance with the existing legal framework governing personal data protection and artificial intelligence. At the same time, public awareness and data literacy should be promoted to enable individuals to understand the implications of data processing and exercise their statutory rights effectively. Integrating these measures into a coherent rights-based regulatory approach would help ensure that technological innovation remains consistent with the protection of fundamental human rights.

Fourthly, improving cross-border data governance and international cooperation. The comparison with EU law highlights the importance of establishing clear, transparent, and legally predictable mechanisms for international personal data transfers. While the GDPR emphasizes the continuity of data protection through adequacy decisions and appropriate safeguards, Vietnam currently places considerable emphasis on cross-border transfer impact assessments and administrative supervision. Accordingly, Vietnam should further clarify the procedures, assessment criteria, exemptions, and regulatory responsibilities applicable to cross-border transfers, ensuring that protective measures remain proportionate to actual risks and do not create unnecessary barriers to legitimate international data flows. In addition, Vietnam should explore opportunities for international regulatory cooperation, including assessing the feasibility of participation in the Global Cross-Border Privacy Rules (Global CBPR) system and other internationally recognized privacy protection initiatives. Such cooperation should complement, rather than replace, domestic legal obligations and the safeguards required under applicable foreign data protection regimes. Strengthening the interoperability of legal standards and regulatory cooperation would contribute to protecting personal data while facilitating international trade, investment, and the sustainable development of Vietnam's digital economy.

## 5. CONCLUSION

The protection of human rights in the data economy requires a comprehensive legal framework supported by effective enforcement mechanisms. The European Union provides a valuable reference through its rights-based approach under the Charter of Fundamental Rights, the GDPR, and the Data Act, which seeks to reconcile personal data protection with digital economic development. In Vietnam, the enactment of the 2025 Law on Personal Data Protection represents significant progress toward strengthening legal safeguards in the digital environment. Nevertheless, effective protection depends not only on legislative recognition but also on institutional oversight, regulatory accountability, and accessible mechanisms for complaints and compensation. Accordingly, Vietnam should strengthen enforcement capacity, enhance transparency, promote public awareness of data protection, and selectively incorporate international best practices to ensure that digital economic development remains consistent with the effective protection of fundamental human rights.

## REFERENCES

1. Mujahid Mohiuddin Babu et al., *Exploring Big Data-Driven Innovation in the Manufacturing Sector: Evidence from UK Firms*, 333 Annals of Operations Research 689 (2024), https://doi.org/10.1007/s10479-021-04077-1.
2. Andrea Armstrong et al., *Everyday Digital Traces*, 10 Big Data & Society 20539517231213827 (2023), https://doi.org/10.1177/20539517231213827.
3. S. C. Matz et al., *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 114 Proceedings of the National Academy of Sciences 12714 (2017), https://doi.org/10.1073/pnas.1710966114.
4. Inge Graef et al., *Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice*, 2 Digital Society 19 (2023), https://doi.org/10.1007/s44206-023-00045-3.
5. Ngoc Tuan Tran, *Human-Centric Approaches to Digital Privacy: Insights from the Europe with Implications for Vietnam*, 13 Social Sciences & Humanities Open 102926 (2026), https://doi.org/10.1016/j.ssaho.2026.102926.
6. Yuliia Kovalenko, *The Right to Privacy and Protection of Personal Data: Emerging Trends and Implications for Development in Jurisprudence of European Court of Human Rights*, 16 Masaryk University Journal of Law and Technology 37 (2022), https://doi.org/10.5817/MUJLT2022-1-2.
7. Vo Trung Hau, *Human Rights and Control of Personal Data in the Digital Economy: EU Legal Case Studies and Recommendations for Vietnam*, 14 Ius Humani. Law Journal 137 (2025), https://doi.org/10.31207/ih.v14i1.409.
8. Bart Custers & Gianclaudio Malgieri, *Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data*, 45 Computer Law & Security Review 105683 (2022), https://doi.org/10.1016/j.clsr.2022.105683.
9. Ana Cristina Bicharra Garcia et al., *Algorithmic Discrimination in the Credit Domain: What Do We Know About It?*, 39 AI & Society 2059 (2024), https://doi.org/10.1007/s00146-023-01676-3.

10. Damian Eke & Bernd Stahl, *Ethics in the Governance of Data and Digital Technology: An Analysis of European Data Regulations and Policies*, 3 Digital Society 11 (2024), https://doi.org/10.1007/s44206-024-00101-6.
11. Uta Kohl, *The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy*, 72 International and Comparative Law Quarterly 737 (2023), https://doi.org/10.1017/S0020589323000258.
12. Paul De Hert et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 Computer Law & Security Review 193 (2018), https://doi.org/10.1016/j.clsr.2017.10.003.
13. Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 International Data Privacy Law 76 (2017), https://doi.org/10.1093/idpl/ipx005.
14. Federico Fabbrini & Edoardo Celeste, *The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders*, 21 German Law Journal 55 (2020), https://doi.org/10.1017/glj.2020.14.
15. Federico Casolari et al., *The EU Data Act in Context: A Legal Assessment*, 31 International Journal of Law and Information Technology 399 (2023), https://doi.org/10.1093/ijlit/eaae005.
16. Pieter Wolters, *The Influence of the Data Act on the Shifting Balance Between Data Protection and the Free Movement of Data*, 15 European Journal of Law and Technology, no. 1, 2024, https://ejlt.org/index.php/ejlt/article/view/991 (last visited Nov. 16, 2026).
17. Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 Nature Communications 3069 (2019), https://doi.org/10.1038/s41467-019-10933-3.
18. Thi Ha Do & Niloufer Selvadurai, *Data Sovereignty and the Digital Economy: Analysing the Effectiveness of Viet Nam's Cyber Security and Cybercrime Laws*, Asian Journal of Law and Society 1 (2026) (published online July 14, 2026), https://doi.org/10.1017/als.2026.10056.
19. Duc Anh Nguyen, *Between Digital Trade Commitments and Sovereignty: Asian Developing Members' Approaches to the CPTPP's Cross-Border Data Transfers*, Asian Journal of Law and Society 1 (2026) (published online Sept. 24, 2026), https://doi.org/10.1017/als.2026.10057.
20. Joanna Strycharz & Claire M. Segijn, *Ethical Side-Effect of Dataveillance in Advertising: Impact of Data Collection, Trust, Privacy Concerns and Regulatory Differences on Chilling Effects*, 173 Journal of Business Research 114490 (2024), https://doi.org/10.1016/j.jbusres.2023.114490.
21. Peter Aagaard & Selma Marthedal, *Political Microtargeting: Towards a Pragmatic Approach*, 12 Internet Policy Review, no. 1 (2023), https://doi.org/10.14763/2023.1.1690.
22. Anh Thu Nguyen, *Processing of Personal Data Without Consent for the Protection of Life and Health in Vietnam: A Comparison with European Union Law*, 3 Social Sciences in Brief 1 (2026), https://doi.org/10.47909/ssb.27.
23. Sandra Seubert & Carlos Becker, *The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection*, 22 German Law Journal 31 (2021), https://doi.org/10.1017/glj.2020.101.
24. Hoang Le Ngoc Tien Dat & Chu Thi Thanh An, *The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam*, 11 Vietnamese Journal of Legal Sciences 1 (2024), https://doi.org/10.2478/vjls-2024-0007.
25. Timo Jakobi et al., *The Role of IS in the Conflicting Interests Regarding GDPR*, 62 Business & Information Systems Engineering 261 (2020), https://doi.org/10.1007/s12599-020-00633-4.
26. European Commission. (2020, November 25). *Commission staff working document: Impact assessment report accompanying the document Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)* (SWD(2020) 295 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0295