

Received: 28.06.2026. Accepted: 30.06.2026. Available online: 30.06.2026.

GRSTI 10.87.01

DOI: <https://www.doi.org/10.32523/2791-0954-2026-18-2-43-58>

**Personal data protection in emerging digital economies:
regulatory convergence and divergence between Vietnam and Kazakhstan
under international data governance standards**

Nguyen Thi Long

Doctor of Philosophy (PhD)

Senior Lecturer, Department of Civil Law, Hanoi Law University, Vietnam

e-mail: longnt@hlu.edu.vn

ORCHID: 0009-0005-3854-4809

Bekmyrza Karazhan

Doctor of Philosophy (PhD)

Senior lecturer of the Department of international law of L.N. Gumilyov ENU

Astana, Kazakhstan

e-mail: karazhan_bs_3@enu.kz

ORCHID: 0000-0002-4927-9634

Abstract. As Vietnam and Kazakhstan deepen their cooperation in trade, investment, and digital transformation, the protection of personal data has become an important legal prerequisite for building digital trust and facilitating cross-border data flows. This article examines and compares the legal frameworks governing personal data protection in the two countries in light of international standards, including the GDPR, the OECD Privacy Guidelines, and the APEC Privacy Framework. Significant differences remain between the two countries in terms of regulatory measures. Vietnam has developed a more comprehensive and rights-oriented framework, whereas Kazakhstan places greater emphasis on data sovereignty and localization. The article argues that stronger accountability mechanisms, improved enforcement, and greater regulatory harmonization are necessary to enhance digital trust and support sustainable digital economic cooperation between the two countries.

Keywords: personal data protection, data subject rights, digital economy, Vietnam, Kazakhstan, comparative law.

**Дамушы цифрлық экономикалардағы жеке деректерді қорғау:
деректерді басқарудың халықаралық стандарттары аясындағы Вьетнам
мен Қазақстан арасындағы реттеу мәселесіндегі ұқсастық пен
айырмашылық**

Нгуен Тхи Лонг

Философия докторы (PhD)

Ханой Заң университетінің азаматтық құқық кафедрасының аға оқытушысы,
Вьетнам

e-mail: longnt@hlu.edu.vn

ORCHID: 0009-0005-3854-4809

Қаражан Бекмырза Серікұлы

Философия докторы (PhD)

Л.Н. Гумилев атындағы ЕҰУ халықаралық құқық кафедрасының аға
оқытушысы

Астана, Қазақстан

e-mail: karazhan_bs_3@enu.kz

ORCHID: 0000-0002-4927-9634

Андатпа. Вьетнам мен Қазақстан сауда, инвестиция және цифрлық трансформация саласындағы ынтымақтастығын арттырумен жеке деректерді қорғау мәселесі цифрлық сенімділікті орнықтыру және трансшекаралық деректер ағындарын оңтайландыру үшін маңызды құқықтық алғышартқа айналды. Бұл мақалада екі елдегі жеке деректерді қорғау ісі халықаралық стандарттар, оның ішінде GDPR, ЭЫДҰ нұсқаулары мен АРЕС ережелері тұрғысынан қарастырылады. Екі ел арасында реттеу шаралары тұрғысынан айтарлықтай айырмашылықтар сақталуда. Вьетнам кешенді және құқыққа бағытталған шеңберді әзірледі, ал Қазақстан деректердің егемендігі мен локализациясына көбірек көңіл бөледі. Мақалада екі ел арасындағы цифрлық сенімді нығайту және тұрақты цифрлық экономикалық ынтымақтастықты қолдау үшін есеп беру механизмдерін, құқық қорғау және нормативтік үйлестіруді күшейту қажет деп тұжырымдалады.

Түйін сөздер: жеке деректерді қорғау, деректер субъектілерінің құқықтары, цифрлық экономика, Вьетнам, Қазақстан, салыстырмалы құқық.

**Защита персональных данных в развивающихся цифровых
экономиках: схожести и различия регулирования между Вьетнамом и
Казахстаном в рамках международных стандартов управления данными**

Нгуен Тхи Лонг

Доктор философии (PhD)

Старший преподаватель, кафедра гражданского права, Ханойский юридический
университет, Вьетнам

e-mail: longnt@hlu.edu.vn

ORCHID: 0009-0005-3854-4809

Каражан Бекмырза Серикович

Доктор философии (PhD)

Старший преподаватель кафедры международного права ЕНУ им.

Л.Н. Гумилёва

Астана, Казахстан

e-mail: karazhan_bs_3@enu.kz

ORCID: 0000-0002-4927-9634

Аннотация. По мере углубления сотрудничества Вьетнама и Казахстана в сфере торговли, инвестиций и цифровой трансформации защита персональных данных стала важной правовой предпосылкой для построения цифрового доверия и облегчения трансграничных потоков данных. В данной статье рассматриваются и сравниваются правовые рамки, регулирующие защиту персональных данных в двух странах, в свете международных стандартов, включая GDPR, Руководящие принципы ОЭСР по защите конфиденциальности и Рамочную программу АТЭС по защите конфиденциальности. Между двумя странами сохраняются существенные различия в отношении нормативных мер. Вьетнам разработал более всеобъемлющую и ориентированную на права человека систему правового регулирования, в то время как Казахстан уделяет больше внимания суверенитету данных и локализации. В статье рассматриваются меры повышения цифрового доверия и поддержки устойчивого цифрового экономического сотрудничества между двумя странами.

Ключевые слова: защита персональных данных, права субъектов данных, цифровая экономика, Вьетнам, Казахстан, сравнительное право.

Introduction

In the digital economy, personal data is processed across various models, ranging from digital platforms, the sharing economy, e-commerce - digital advertising, fintech, digital government, and smart cities to the data economy models, creating a large and complex ecosystem. Digital platforms and the sharing economies collect behavioral, location and transaction data to optimize services, but come with the risk of abuse, tracking and information leakage. E-commerce and digital advertising process data via cookies and device identification to personalize advertising but easily lead to excessive collection and sharing of data through multiple intermediaries. In digital finance (fintech), sensitive data such as identification and transactions are analyzed by AI to assess creditworthiness, but there is a potential risk of account loss or identity theft. Digital governments store and integrate large amounts of citizen data to improve public services, but weak security could result in large-scale data leakage. At the same time, IoT (Internet of Things) and smart cities use data from sensors and connected devices, bringing convenience but increasing the risk of cyber-attacks and invasion of privacy. Finally, in the data economy model, personal data becomes an asset for analysis and transaction, and while it holds economic value, it constantly faces the risk of re-identification and legal conflicts when transferred across borders.

The object of the study is the legal system and the mechanism for enforcing regulations on personal data protection in Vietnam and Kazakhstan. The research theme focuses on the degree of compatibility and potential for harmonization between these two legal systems and international standards. The goal of the research is to demonstrate that establishing a transparent, modern framework for personal data protection consistent with international practice will contribute to enhancing data governance efficiency, reinforcing user trust, and promoting digital economic cooperation between the two nations. It hypothesizes that while the legal frameworks of both countries have made significant progress, a gap remains compared to international standards, necessitating more harmonized and practical solutions.

Research gap and research questions. Personal data protection has become a central issue in contemporary digital law scholarship. Issues such as data subject rights, cross-border data flows, accountability mechanisms and data governance challenges in the digital economy have been addressed in detail in other studies. At the international level, significant attention has also been devoted to the regulatory influence of the GDPR, the OECD Privacy Guidelines, and the APEC Privacy Framework.

Despite this growing body of literature, comparative research between Southeast Asian and Central Asian jurisdictions remains limited. In particular, the protection of personal data subjects in Vietnam and Kazakhstan has received little scholarly attention, notwithstanding both countries' ongoing digital transformation, expanding digital economies, and increasing engagement with international data governance standards. Moreover, existing studies tend to assess individual legal systems separately, while insufficient attention has been paid to how emerging digital economies adapt and localize international data protection principles within different institutional and governance contexts.

Against this background, this article conducts a comparative analysis of the legal frameworks governing the protection of personal data subjects in Vietnam and Kazakhstan in light of international standards. The study addresses three research questions: (i) To what extent are the legal frameworks of Vietnam and Kazakhstan compatible with international standards on personal data protection? (ii) What are the principal similarities and differences in the protection of data subject rights and related enforcement mechanisms? and (iii) What legal reforms are necessary to enhance regulatory harmonization, digital trust, and digital economic cooperation between the two jurisdictions?

Beyond a descriptive comparison, the article argues that Vietnam and Kazakhstan represent two distinct approaches to adapting international data protection standards, reflecting different governance priorities and regulatory strategies in emerging digital economies.

Materials and methods

This research employs a comparative legal research methodology combined with an interdisciplinary approach grounded in digital economy theory, data governance, and international human rights standards. The study primarily focuses on examining

the legal frameworks governing the protection of personal data subjects in Vietnam and Kazakhstan within the context of rapid digital economic transformation.

The research materials consist of domestic legal instruments, international legal frameworks, academic literature, institutional reports, and policy documents. The primary domestic sources include the 2025 Law on Personal Data Protection of Vietnam, Decree No. 356/2025/NĐ-CP, the Constitution of Vietnam 2013, the Civil Code of Vietnam 2015, the Law of the Republic of Kazakhstan “On Personal Data and Their Protection” (2013), the Law “On Informatization” (2015), the Digital Code of Kazakhstan (2026), and relevant constitutional and criminal law provisions. International materials include the General Data Protection Regulation (GDPR), the OECD Privacy Guidelines, the APEC Privacy Framework, and the United Nations Convention against Cybercrime 2024.

The study applies several research methods. First, the doctrinal legal analysis method is used to examine legal principles, rights of data subjects, obligations of data processors, enforcement mechanisms, and limitations on personal data processing in both jurisdictions. Second, the comparative method is employed to identify similarities, differences, and levels of compatibility between the Vietnamese and Kazakhstani legal systems and international standards. Third, a policy-analysis approach is adopted to assess the practical implementation of personal data protection through selected examples from digital platforms, fintech institutions, and e-commerce enterprises.

In addition, the research incorporates qualitative analysis of practical cases relating to data breaches, cybersecurity incidents, and digital governance challenges in order to evaluate the effectiveness of current legal mechanisms in practice. The study also considers broader socio-economic and institutional factors influencing the development of personal data protection frameworks in emerging digital economies.

The scope of the research is limited to issues relating to personal data protection in the digital economy and does not comprehensively address broader cybersecurity or national defense regulations, except where such issues directly affect the rights of personal data subjects.

Results and discussion

Unlike previous studies that primarily focus either on the European Union’s GDPR framework or on single-country legal analysis, this study adopts a comparative and interdisciplinary approach to examine two emerging digital economies that have received limited scholarly attention in the field of data governance.

The analysis highlights how rapid digital transformation has reshaped the legal understanding of personal data from a private informational interest into a strategic economic and governance resource. In this context, the study explores the interaction between international legal standards, domestic regulatory reforms, and practical implementation challenges in both countries. Particular attention is paid to the convergence and divergence of the legal frameworks of Vietnam and Kazakhstan in relation to international principles such as the GDPR, the OECD Privacy Guidelines, and the APEC Privacy Framework.

The research results demonstrate that, while both countries are moving toward stronger personal data protection regimes, their regulatory approaches differ significantly in terms of institutional structure, enforcement mechanisms, state involvement, and the balance between data sovereignty and the free flow of information. Through the comparative analysis method, the study contributes to the broader academic debate on data governance in developing digital economies and offers policy-oriented recommendations aimed at strengthening legal harmonization, digital trust, and bilateral digital economic cooperation between Vietnam and Kazakhstan.

International legal regulation of the protection of the rights of personal data subjects in the digital economy

Foundational international instruments, including the Universal Declaration of Human Rights (1948), the European Convention on Human Rights (1950), and the International Covenant on Civil and Political Rights (1966), recognize the importance of privacy and the protection of individuals against unlawful interference with their private lives. These principles provide the normative basis for the development of modern personal data protection regimes. In contemporary digital governance, personal data protection is increasingly regarded not merely as an extension of the right to privacy but as an autonomous legal interest requiring distinct regulatory safeguards, accountability mechanisms, and cross-border governance frameworks [1].

At the international level, several specialized instruments have established standards for the protection of personal data. One of the earliest and most influential is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which entered into force in 1985. The Convention introduced key principles governing the lawful processing of personal data and was significantly modernized through Protocol No. 223 in 2018 to address challenges arising from digitalization, artificial intelligence, and cross-border data processing [2].

Another influential instrument is the European Union's General Data Protection Regulation (GDPR), which has become a global benchmark for personal data protection. The GDPR establishes a comprehensive framework based on principles such as lawfulness, transparency, purpose limitation, accountability, and data security. It also recognizes a wide range of data subject rights, including the rights of access, rectification, erasure, data portability, and notification in the event of data breaches. Beyond the European Union, the GDPR has significantly influenced legislative reforms in many jurisdictions [3].

In addition, the OECD Privacy Guidelines provide an important framework for balancing privacy protection with the free flow of information across borders. Although not legally binding, the Guidelines have played a significant role in shaping national data protection policies and promoting international cooperation in cross-border data governance [4].

A further regional framework is the APEC Privacy Framework, which adopts a business-oriented and trade-facilitating approach to personal information protection.

Unlike the GDPR, which places data subjects at the center of the regulatory framework, the APEC model focuses on organizational accountability and the promotion of cross-border data flows. Nevertheless, it recognizes core rights such as notice, choice, access and correction, security safeguards, and remedies, while seeking to balance privacy protection with digital commerce [5].

More recently, the United Nations Convention against Cybercrime (2024) has reinforced the international legal framework by recognizing the importance of personal data protection in international cooperation against cybercrime. Article 36 of the Convention requires that the transfer of personal data be conducted in accordance with domestic law and applicable international obligations relating to personal data protection. The Convention therefore reflects the growing recognition that effective cybersecurity and personal data protection are mutually reinforcing objectives in the digital age [6].

Taken together, Convention 108+, the GDPR, the OECD Privacy Guidelines, the APEC Privacy Framework, and the UN Convention against Cybercrime constitute the principal international standards relevant to personal data protection. These instruments provide the analytical benchmark for assessing the legal frameworks of Vietnam and Kazakhstan in this study [7].

The impact of international standards on the policies of Vietnam and Kazakhstan

The impact of the international legal framework on personal data protection in Vietnam and Kazakhstan is a profound example of regulatory transplanting within the digital economy. As both nations transition into data-driven ecosystems, they have increasingly looked toward global benchmarks, most notably the GDPR, the APEC Privacy Framework, and the OECD Guidelines, to bridge the gap between rapid technological innovation and legislative oversight, that allow these nations to participate in global trade while safeguarding the fundamental rights of their citizens.

The GDPR, as the gold standard of data sovereignty, has significantly influenced the architecture of Vietnam's Decree 13/2023 and the subsequent Law on Personal Data Protection (2025). By adopting GDPR principles such as purpose limitation, data minimization, and the requirement for explicit consent, Vietnam has elevated the status of the data subject from a passive participant to an active controller of their digital identity. This alignment is not only an academic exercise but also a strategic economic necessity. In the digital economy, adherence to international standards reduces friction in cross-border trade and fosters digital trust, which is essential for attracting foreign direct investment (FDI) from tech giants accustomed to high compliance environments. In Kazakhstan, the influence of the GDPR is most visible within the Astana International Financial Centre (AIFC). By adopting GDPR regulations, the AIFC ensures that international investors and data subjects interact within a privacy safe environment.

The APEC Privacy Framework has been instrumental in shaping how Vietnam and Kazakhstan handle the movement of data across borders in the modern digital economy. Vietnam, as an APEC member, has integrated the accountability and

preventing harm principles into the 2026 Personal Data Protection Law. Kazakhstan, while not an APEC member, has observed these regional trends to refine its own cross-border mechanisms, that facilitates smoother integration into the global digital economy.

The OECD Guidelines have served as a critical normative benchmark for both Vietnam and Kazakhstan. For Vietnam, the OECD's accountability principle is the cornerstone of the 2026 Law on Personal Data Protection, which mandates that organizations demonstrate compliance through compulsory data protection impact assessments. Similarly, OECD Guidelines have provided a pragmatic roadmap for Kazakhstan as it develops its Digital Code.

However, the impact of these frameworks is often mediated by national interests. In Vietnam, international norms are integrated with a strong emphasis on data localization and national security, creating a stringent compliance regime, while Kazakhstan is relatively more permissive stance. The international legal framework acts as a gravitational force, pulling both nations toward unified standards that protects data subjects while providing the legal certainty required for a competitive, globalized digital economy that create a prerequisite for sustainable economic growth.

Legal Framework for Protecting the Rights of Personal Data Subjects and Implementation Practices in Vietnam

Fundamental Regulations. In Vietnam, rights relating to personal data are implicitly recognized in Article 21 of the 2013 Constitution, which guarantees the inviolability of private life, personal and family secrets, and the confidentiality of personal information [8]. These constitutional guarantees are further specified in Article 38 of the 2015 Civil Code, which affirms the right to privacy and explicitly requires an individual's consent for the collection, storage, use, and disclosure of information concerning private life, personal secrets, and family secrets. At the same time, both the Constitution and the Civil Code impose corresponding obligations on other subjects to respect and protect these rights and to refrain from unlawful interference [9].

Beyond constitutional and civil law protections, personal data protection in Vietnam is also embedded within a broader framework of cybersecurity and digital governance. The Law on Cybersecurity 2018 imposes obligations on domestic and foreign organizations providing services in cyberspace to ensure information security, prevent cyber threats, and cooperate with competent authorities in safeguarding national cybersecurity interests. Although the Law on Cybersecurity is not a dedicated personal data protection statute, it plays an important role in regulating the collection, storage, transmission, and protection of information in cyberspace [10]. Consequently, Vietnam's legal framework for personal data protection should be understood as a multi-layered system consisting of constitutional guarantees, civil law remedies, cybersecurity safeguards, and specialized personal data protection legislation.

The mechanisms for protecting the rights of personal data subjects are prescribed indirectly, primarily through the Civil Code 2015, which provides a general framework for the protection of civil rights, including those related to personal data. Articles 11 to

15 of the Civil Code establish various methods for protecting civil rights. These methods may be divided into two groups. The first consists of self-protection measures, allowing individuals to take necessary actions to protect their lawful rights and interests, provided that such measures are proportionate and consistent with the fundamental principles of civil law. The second consists of remedies through competent authorities and organizations, including judicial protection by the courts. Importantly, Vietnamese courts are not permitted to refuse to adjudicate a civil dispute merely because there is no directly applicable legal provision, thereby providing an additional safeguard for emerging rights relating to personal data [9].

Another important mechanism concerns the lawful limitation of rights. Pursuant to Article 14(2) of the Constitution and Article 2(2) of the Civil Code, human rights and civil rights, including rights relating to personal data, may be restricted only by law and only where necessary for reasons of national defense, national security, social order and safety, social morality, or community well-being.

In conclusion, Vietnam has developed a multi-layered legal framework for the protection of personal data. At the constitutional level, privacy and personal information are recognized as fundamental rights. At the civil law level, individuals are provided with legal remedies and mechanisms for the protection of their lawful interests. At the cybersecurity level, the Law on Cybersecurity establishes safeguards relating to information security and national cybersecurity. These foundations have subsequently supported the development of a specialized personal data protection regime.

General and Specific Provisions. The primary legal instruments governing personal data protection in Vietnam are the Law on Personal Data Protection No. 91/2025/QH15 and Decree No. 356/2025/ND-CP, which provides detailed provisions for its implementation. According to Article 2(4) of the Law, personal data protection refers to the use of measures, resources, and mechanisms by agencies, organizations, and individuals to prevent and address infringements of personal data [11].

A notable feature of the 2025 Law is its explicit recognition of the rights of personal data subjects. Article 4 grants individuals a broad range of rights, including the right to be informed of data processing activities, the right to consent and withdraw consent, the right to access and rectify personal data, the right to request deletion or restriction of processing, the right to object to processing, and the right to seek remedies through complaints, litigation, and compensation mechanisms. These rights significantly strengthen individual control over personal data and reflect Vietnam's increasing convergence with internationally recognized data protection standards.

Cross-border data transfers constitute another important component of the Vietnamese framework. Article 20 of the Law recognizes the legality of cross-border transfers of personal data, while Decree No. 356/2025/ND-CP establishes detailed requirements regarding transfer agreements, security measures, risk assessments, and transfer impact assessment reports. Organizations transferring personal data abroad must evaluate risks associated with overseas processing, identify mitigation measures, and maintain documentation for regulatory review. Additional safeguards, including

encryption, anonymization, and physical security measures, are required when transferring sensitive personal data [11].

The Law further regulates personal data protection in specific sectors closely associated with the digital economy, including finance, banking, credit, advertising services, online communication services, and biometric data processing. These sector-specific provisions generally combine general data protection obligations with additional safeguards tailored to the characteristics and risks of particular activities.

To ensure effective implementation, the Law and its implementing Decree establish several enforcement mechanisms. Organizations are required to maintain compliance programs, monitor non-consensual processing activities, conduct impact assessments, and cooperate with supervisory authorities. Furthermore, Decree No. 356/2025/ND-CP introduces detailed breach notification requirements, obliging organizations to report personal data protection violations and provide information regarding the nature of the breach, affected data, potential consequences, and remedial measures undertaken [12].

Overall, the 2025 Law on Personal Data Protection and Decree No. 356/2025/ND-CP represent a significant development in Vietnam's data governance regime. Together with constitutional guarantees, civil law remedies, and cybersecurity safeguards, these instruments form an increasingly comprehensive and coherent legal framework that seeks to balance the protection of personal data, digital innovation, national security, and the sustainable development of the digital economy.

Vietnam has demonstrated a strong commitment to digital transformation through Decision No. 1033/QĐ-TTg approving the Programme for Digital Economy and Digital Society Development for the Period 2026–2030 [13]. The Programme targets the digital economy to contribute approximately 30% of GDP by 2030, with 100% of citizens aged 14 and above possessing digital identification accounts and 99% of the population covered by 5G networks, while promoting national databases, data-sharing mechanisms, and AI-driven services as foundations of a data-driven economy [14].

Legal framework for protecting the rights of personal data subjects and implementation practices in Kazakhstan

In the Republic of Kazakhstan, the protection of personal data is ensured by the Constitution, the Law of May 21, 2013, "On Personal Data and Their Protection," the Law of November 24, 2015, "On Informatization," the Digital Code of the Republic of Kazakhstan, and a number of other regulatory legal acts.

It should be noted that in the new Constitution, adopted at a national referendum on March 15, 2026, this article was amended to Article 21 and reads as follows: "The right to privacy, personal and family secrets, and the protection of personal data from illegal collection, processing, storage, and use, including through the use of digital technologies, is guaranteed by law" [15]. As can be seen, the article has been supplemented with a provision that takes into account the modern realities of social relations – it mentions the use of digital technologies. The new Constitution will come into force on July 1, 2026.

The Civil Code of the Republic of Kazakhstan classifies privacy, personal and family secrets as personal non-property benefits and rights [16].

The primary law in the field of personal data protection in Kazakhstan is the Law of the Republic of Kazakhstan dated May 21, 2013, "On Personal Data and Its Protection." This law defines the concept of "personal data protection." According to paragraph 11 of Article 1 of the law, personal data protection is a set of measures, including legal, organizational, and technical ones, implemented for the purposes established by this law [17].

The purpose of the Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V "On Personal Data and their protection" is to ensure the protection of human and civil rights and freedoms during the collection and processing of personal data.

Article 3 of the Law states that it regulates "relations related to the collection, processing and protection of personal data".

Article 9 of the Law provides for the possibility of collecting and processing personal data without the consent of the subject. At the same time, he explains the circumstances in which this is possible, which he refers to as cases of "carrying out the activities of law enforcement agencies, courts and other authorized state bodies", carrying out activities in the field of statistics; maintaining military records; implementing international treaties of Kazakhstan; the need to protect the stipulated The Constitution of the Republic of Kazakhstan on human rights and freedoms; implementation by the unified accumulative pension fund of activities for special types of activities; carrying out the activities of a journalist within the framework of his profession and media activities for the protection of human rights; publishing personal data of candidates for elected positions of the state; transferring backup copies containing personal data of limited access; using personal data of a Kazakhstani citizen when submitting an application for the application of an out-of-court or judicial bankruptcy procedure.

Article 11 ensures the confidentiality of personal data of citizens. "Accumulation of personal data," as stated in article 12 of this Law, "is carried out by collecting personal data necessary and sufficient to perform tasks performed by the owner and (or) operator, as well as by a third party." We should agree with F. Syrlybayeva, K. Kasymova and other authors who claim that "the obligations of the employer are not established at the state level" and there is no clear mechanism for "ensuring the confidentiality of personal data of employees" [18, p. 90-91].

If in Article 12 (part 2) of the Law of the Republic of Kazakhstan "On Personal Data" "personal data is stored by the owner and (or) the operator, as well as by a third party in a database located on the territory of the Republic of Kazakhstan", in Article 18 of the Law of Vietnam dated June 26, 2025 there is no such strict requirement and in this regard it He speaks about the need to create convenience for Vietnamese businesses. It follows that the personal data of Vietnamese citizens can be located both within the country and abroad.

Article 16 of the Law defines the cross-border transfer of personal data as the transfer of "personal data to the territory of foreign States." Article 17 of the Law draws

attention to the fact that the collection and processing of personal data for the national artificial intelligence platform in order to depersonalize personal data of citizens is carried out by the operator of the national artificial intelligence (AI) platform in accordance with the data management requirements approved by the Kazakh Government. In a scientific article by R.D. Akshalova and M. Iqbal outlined the connection between artificial intelligence and cybernetics related to personal electronic data [19, pp. 57-58].

While in Europe, according to article 15 of the General Data Protection Regulation, personal data subjects have broad rights, including access to their data, the right to correct inaccuracies (article 16 of the General Regulation), and the right to data portability (under article 20 of the General Regulation), "in Kazakhstan, the rights of personal data subjects are more limited" (see Article 19 of the Law of the Republic of Kazakhstan "On Personal Data and their Protection). Based on the conclusion of these authors, we propose to expand the rights of Kazakhstani citizens for wider access to their personal data.

A separate chapter 3 of the Law is devoted to the protection of personal data of citizens of the republic. Article 20 of the Law guarantees the protection of personal data with the help of the State. What is the meaning of personal data protection purposes? The answer to this question is provided by article 21 of the Law, which assumes that such protection is carried out in order to: exercise "privacy rights"; preserve their integrity; respect them in confidentiality; exercise the right to access them; prevent illegal collection and processing of this data. In this chapter, much attention is paid to the protection of electronic information resources that contain personal data.

In chapter 4, based on Article 24, a personal data subject has the right to: "know about the availability of their personal data from the owner and (or) operator, as well as a third party", "require the owner and (or) operator, as well as a third party, to block their personal data in case of information about a violation of the terms of collection, processing of personal data".

Another significant difference between the Vietnamese law and the Kazakh law is that while article 8 of the Vietnamese Law provides for sufficiently severe sanctions for violating the norms of the Law on Personal Data, the Kazakh law does not provide for penalties in accordance with article 29. The Kazakh legislator focused on punishments for similar violations in the administrative law (article 79 of the Code of Administrative Offences of the Republic of Kazakhstan: recently, fines for violations of the legislation on personal data awarded by administrative courts have been increased) and criminal law (article 147 of the Criminal Code of the Republic of Kazakhstan). The reader can learn more about the issues of liability for violations of personal data laws in Europe and Asia (using Indonesia as an example) from the scientific article by D. Pavestri, A. Kusumadara and others on the subject [20].

Regulatory Convergence and Divergence between Vietnam and Kazakhstan

The comparative analysis demonstrates that the personal data protection frameworks of Vietnam and Kazakhstan exhibit both convergence and divergence in

relation to internationally recognized standards, particularly those reflected in the GDPR, the OECD Privacy Guidelines, and the APEC Privacy Framework. While both jurisdictions increasingly recognize personal data protection as a fundamental component of digital governance and digital trust, they have adopted different regulatory approaches in implementing these principles. Vietnam has developed a more comprehensive rights-based framework under the 2025 Law on Personal Data Protection, while Kazakhstan continues to strengthen its legal framework through ongoing legislative modernization and digital governance reforms.

Differences become more apparent in the areas of cross-border data governance and data localization. Vietnam permits cross-border transfers subject to regulatory safeguards and compliance requirements, reflecting a relatively flexible and accountability-oriented approach. Kazakhstan, by contrast, adopts a more controlled model that places greater emphasis on regulatory oversight, data security, and the localization of personal data within national territory.

Institutional governance and enforcement mechanisms also reveal divergent regulatory priorities. Vietnam has strengthened compliance obligations and sanctions under its new legal framework, while Kazakhstan relies primarily on administrative and criminal liability mechanisms supported by state-centered regulatory oversight. These approaches reflect different understandings of how personal data protection should be balanced against national security, regulatory control, and digital economic development.

Overall, the comparison suggests that convergence with international standards does not necessarily result in regulatory uniformity. Rather, Vietnam and Kazakhstan illustrate how emerging digital economies adapt global data protection principles to their respective legal traditions, governance priorities, and socio-economic contexts. This process may be better understood as adaptive harmonization, whereby international standards are localized while preserving distinctive national regulatory characteristics.

Criteria	GDPR	Vietnam	Kazakhstan
Data subject rights	Comprehensive	Broadly aligned	More limited
Accountability mechanisms	Strong	Strong	Developing
Cross-border data transfers	Adequacy-based	Conditional	Controlled
Data localization	No general requirement	Partial	Strong
Supervisory model	Independent Authority	Ministry-based	State-based
Enforcement mechanisms	Comprehensive	Strengthening	Developing
Regulatory orientation	Rights-based	Accountability-oriented	Sovereignty-oriented

*Table 1. Comparative Assessment of Vietnam and Kazakhstan
(compiled by the authors)*

Towards greater harmonization of personal data protection frameworks in Vietnam and Kazakhstan

Although Vietnam and Kazakhstan have made significant progress in developing legal frameworks for personal data protection, further efforts are needed to promote regulatory harmonization and facilitate digital economic cooperation.

1) Different Regulatory Priorities: Vietnam has increasingly emphasized accountability, compliance mechanisms, and risk-based governance, particularly through the 2025 Law on Personal Data Protection. Kazakhstan, meanwhile, places greater emphasis on data security, regulatory oversight, and the protection of national data infrastructure. Greater mutual understanding of these approaches may contribute to future regulatory compatibility.

2) Cross-Border Data Governance and Institutional Development: The growth of digital trade and cross-border digital services requires effective mechanisms for the secure transfer of personal data. Both Vietnam and Kazakhstan continue to strengthen institutional capacity to respond to increasingly complex data governance issues. Enhanced regulatory dialogue and capacity-building initiatives could support greater consistency in implementation.

3) Strengthening Enforcement and Digital Trust: Effective personal data protection depends not only on legislation but also on enforcement and public trust. Strengthening these mechanisms will contribute to building digital trust and supporting sustainable digital economic cooperation between Vietnam and Kazakhstan.

Overall, despite differences in regulatory approaches, both countries share common objectives of protecting personal data, promoting digital trust, and supporting digital economic development. Continued legal reform and regulatory cooperation may therefore provide a foundation for greater harmonization with international standards and more effective cross-border data governance.

Conclusion

The study demonstrates that both Vietnam and Kazakhstan have made significant progress in developing legal frameworks for personal data protection and are increasingly aligned with international standards reflected in the GDPR, the OECD Privacy Shield Guidelines, and the APEC Privacy Shield Framework. However, important differences remain in terms of regulatory priorities, institutional governance, cross-border data flows, and enforcement mechanisms. While Vietnam pursues a more accountability-oriented approach, Kazakhstan places greater emphasis on data sovereignty and regulatory oversight. A comparative analysis suggests that convergence with international standards does not necessarily lead to regulatory uniformity. Rather, developing digital economies are adapting global data protection principles to suit their domestic governance priorities and socioeconomic context. Therefore, strengthening accountability, enforcement capacity, and cross-border regulatory cooperation will be essential for enhancing trust in digital technologies and supporting sustainable digital economic cooperation between Vietnam and Kazakhstan.

References

1. Universal Declaration of Human Rights, GA Res 217 A (III), UN Doc A/810 (1948), art 12; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), ETS No 5 (1950), art 8; International Covenant on Civil and Political Rights, 999 UNTS 171 (1966), art 17; Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7–8.
2. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No 108 (1981); Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No 223 (2018) (Convention 108+).
3. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1; Lee A Bygrave, ‘The GDPR and the Architecture of Accountable Governance’ (2024) 40(1) Computer Law & Security Review.
4. OECD, The OECD Privacy Framework (OECD Publishing 2013), incorporating the 2013 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
5. Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework (2015); Graham Greenleaf and Bertil Cottier, ‘Asian Data Privacy Laws in the Era of Sovereignty and AI: 2024 Update’ (2024) 180 Privacy Laws & Business International Report 18–23.
6. UNGA, ‘United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes’ (24 December 2024) UN Doc A/RES/79/243, art 36.
7. Christopher Kuner, ‘The Sovereignty of Data: Transnational Data Flows in a Fragmented World’ (2024) International Data Privacy Law; Lee A Bygrave, Data Privacy Law: An International Perspective (Oxford University Press 2014).
8. Constitution 2013 (Consolidated Text No 52/VBHN-VPQH, 2025), art 21
9. Civil Code No 91/2015/QH13, art 38.
10. Law on Cybersecurity No 24/2018/QH14, arts 16, 17 and 26.
11. Law on Personal Data Protection No 91/2025/QH15
12. Decree No 356/2025/ND-CP Detailing a Number of Articles and Implementation Measures of the Law on Personal Data Protection, art 28.
13. Prime Minister of Vietnam, Decision No 1033/QĐ-TTg Approving the Programme for Digital Economy and Digital Society Development for the Period 2026–2030 (9 June 2026).
14. Government News, ‘Building a Dynamic Digital Economy Based on Digital Platforms, Data and Artificial Intelligence’ (Government News Portal, 11 June 2026), link: <https://baochinhphu.vn/xay-dung-nen-kinh-te-so-nang-dong-dua-tren-nen-tang-so-du-lieu-va-ai-102260611165534744.htm>, date of access: 12.06.2026

15. Constitution of the Republic of Kazakhstan // Legal information system of Regulatory acts of the Republic of Kazakhstan “Әділет”. URL: https://adilet.zan.kz/rus/docs/K950001000_ (date of access: 20.04.2026)

16. Civil Code of the Republic of Kazakhstan // Legal information system of Regulatory acts of the Republic of Kazakhstan “Әділет”. URL: https://adilet.zan.kz/eng/docs/K940001000_ (date of access: 20.04.2026)

17. On Personal Data and their Protection // Legal information system of Regulatory acts of the Republic of Kazakhstan “Әділет”. URL: <https://adilet.zan.kz/eng/docs/Z1300000094/compare> (date of access: 20.04.2026)

18. Syrlybayeva, Fatima and Kasymova, Ksenia and Omarova, Elmira and Zhussipova, Bakyt and Nurgalieva, Enlik. (2024). Protection of information about personal data of employees in the Republic of Kazakhstan. Socio-legal research. 7. 90-102. 10.32518/sals4.2024.90.

19. Akshalova R.D., Ikbol M. Subjects of intellectual property rights to intellectual property created by artificial intelligence // Eurasian Journal of International Law. 2024. No. 1 (9). Pp. 54-62.

20. Pavestri, Diah and Kusumadara, Afifa and Vidhiyanti, Hanif and Devantara, River. (2025). Administrative liability for data leakage: ensuring the right to compensation in Indonesia and the EU. Legislation. Human. Environment. 16. 173-190. 10.31548/law/3.2025.173.

Authors' contributions

The article was co-authored by a Vietnamese and Kazakh scholar.

1) Nguyen Thi Long analyzed Vietnamese legislation, conducted a comparative analysis, and put forward proposals for improving bilateral cooperation and harmonization of legislations.

2) Bekmyrza Karazhan analyzed Kazakhstani legislation, discussed its compliance with international standards, and examined the similarities and differences between the two laws.