 ***DOI:** https://doi.org/10.63108/IJLMH.12785*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

Ensuring the Protection of Personal Data in the Use of Cloud Computing Services: Legal Obligations and Responsibilities of Relevant Stakeholders

VŨ THỊ NGỌC MAI*

ABSTRACT

In line with the global digital transformation trend, economic organisations and State management agencies are increasingly moving data to cloud platforms because of significant advantages such as lower costs, faster deployment and execution, and substantial improvements in employee productivity. In the context of data being stored across multiple countries, the involvement of numerous intermediaries, and the growing risk of cyberattacks, clearly defining the legal obligations and liabilities of actors throughout the cloud computing service supply chain has become an urgent requirement. Based on an assessment of the current legal framework in Vietnam, the author identifies legal gaps concerning the allocation of liability, cross-border data flow governance, and mechanisms for compensation for damage. On that basis, the article proposes solutions for improving the legal framework so as to balance the objectives of digital economic development and the protection of fundamental human rights.

Keywords: *Cloud computing, Personal data, Legal liability, Civil liability, Personal data protection law*

I. INTRODUCTION

The development of the Fourth Industrial Revolution has brought fundamental changes to the ways in which data are managed, exploited, and used worldwide. Amid the expansion of the digital economy and the global digital transformation trend, data have become a strategic resource driving innovation and economic growth. To optimise the exploitation of this resource, economic organisations, enterprises, and State management agencies in Vietnam are increasingly moving data and information technology systems to cloud computing platforms. This shift is not merely a technological choice but an economic and operational imperative, owing to significant advantages including lower upfront infrastructure investment costs, faster project deployment and implementation, flexible scalability in response to demand, and, in

* Author is an Assistant at the Faculty of Law, Vietnam Women's Academy, Hanoi, Vietnam. ORCID: https://orcid.org/0009-0003-0644-1229

 [ISSN 2581-5369]

particular, enhanced workforce productivity through remote connectivity at any time and from any place.

In Vietnam, cloud computing has been identified as a key priority in the national digital infrastructure strategy and as the backbone for building a digital government, a digital economy, and a digital society. Vietnam's national digital transformation programme identifies three pillars of comprehensive digital transformation: digital government, digital economy, and digital society. The Government has promulgated the Strategy for Development of E-Government Toward Digital Government for the 2021 to 2025 period, with a vision to 2030. One of the tasks and solutions for developing digital government is to restructure the information technology infrastructure of ministries, sectors, and localities and transform it into digital infrastructure using cloud computing technology, so as to connect and manage State-agency resources and data in a secure, flexible, stable, and efficient manner. However, transferring data to the cloud also presents significant challenges to information security and privacy. The technical complexity inherent in cloud service models, that is, infrastructure as a service, platform as a service, and software as a service, makes it particularly difficult to determine roles accurately and to delineate clearly the legal obligations and responsibilities of the data controller, the data processor, and any third party.

This article focuses on the legal framework and the practical implementation of personal data protection in the use of cloud computing services within the context of digital transformation in Vietnam. By examining the technical and legal characteristics of cloud computing, the article clarifies the rights of data subjects, as well as the obligations and legal responsibilities of service providers, service-using organisations, and State authorities. Based on recent legislation, including the 2024 Law on Data and the 2025 Law on Personal Data Protection, the author identifies existing legal gaps and proposes measures to improve the legal framework, with a view to striking an appropriate balance between technological innovation and the protection of privacy rights.

II. General overview of personal data protection and cloud computing

A. Concepts and characteristics of cloud computing

According to the standard definition of the United States National Institute of Standards and Technology, a definition that is widely recognised globally and has provided important guidance for the development of Vietnamese law, cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources

 [ISSN 2581-5369]

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] Accordingly, cloud computing can be understood as a model that enables users, organisations, and businesses to access information technology resources in the form of services, allowing them to select services flexibly on demand while optimising investment costs in information technology infrastructure.[2]

The Ministry of Information and Communications of Vietnam defines cloud computing as a service model that enables the use of shared computing resources, including networks, servers, storage, applications, and services, through network connectivity. These cloud computing resources may be provisioned or terminated by users without requiring intervention from the service provider.[3]

Cloud computing may therefore be understood as a service-delivery model that enables users to exploit, store, process, and share data in a digital environment established between customers and service providers. It helps optimise technology investment costs for storing information and data during operations. In the development of digital government, cloud computing is not merely a technical solution but also core infrastructure for connecting national databases, sharing data among State agencies, and developing online public services for citizens and enterprises.

All cloud computing services share five basic characteristics:

- *On-demand self-service.* Users can provision computing resources automatically, such as servers and storage, without requiring human intervention from the service provider.
- *Broad network access.* Capabilities are available over the network and accessible through standard mechanisms using various devices, such as laptops, tablets, and mobile telephones.
- *Resource pooling.* The provider's computing resources are pooled to serve multiple customers using a multi-tenant model, and resources are dynamically allocated and reallocated according to demand.

[1] NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (Special Publication No. 800-145, 2011).
[2] Vu Thi Luu, Tran Thi Thu Huyen & Nguyen Thi Huyen, *Overview of Cloud Computing and Security Challenges*, VIETNAM J. OF AGRIC. SCIS. (2024), https://tapchi.vnua.edu.vn/wp-content/uploads/2024/10/tap-chi-so-10.13.pdf.
[3] MINISTRY OF INFO. & COMMC'NS, *Guidelines on the Set of Criteria and Technical Indicators for Assessing and Selecting Cloud Computing Platforms Serving Electronic Government*, ch. 2, issued with Official Letter No. 1145/BTTTT-CATTT (Apr. 3, 2020) (Vietnam).

 [ISSN 2581-5369]

- *Rapid elasticity.* Resources can be scaled up or down quickly, and sometimes automatically, to meet demand. This ensures sufficient capacity during traffic peaks while avoiding costs for idle resources in quieter periods.
- *Measured service.* Cloud systems automatically control and optimise resource usage. Usage is monitored, controlled, and reported, providing transparency for both the provider and the consumer, and the consumer pays only for what is used.[4]

B. Concept of personal data

The rapid development of the digital economy and of digital transformation has fundamentally changed perceptions of the value of personal data. Whereas personal data were previously regarded primarily as information serving administrative management or civil transactions, data are now a form of digital asset with significant economic, commercial, and strategic value.

Under article 4 of the General Data Protection Regulation, personal data is defined as "any information relating to an identified or identifiable natural person". A natural person is considered identifiable where he or she can be identified, directly or indirectly, by reference to information such as a name, an identification number, location data, an online identifier, or one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural, or social identity.[5] The Regulation emphasises the possibility of indirect identification, meaning that even where a particular piece of information is insufficient to establish an individual's identity, the combination of multiple data sources may nevertheless enable the data subject to be accurately identified. This characteristic is particularly significant in the cloud computing environment, where data may be distributed across multiple systems but can readily be linked through modern data analytics tools. The Regulation treats personal data as an object requiring protection throughout the entire data-processing lifecycle, from collection, storage, use, and sharing to deletion, rather than limiting protection to the point of collection, as is the case under many traditional legal systems.

In Vietnam, the concept of personal data was first comprehensively regulated under Decree No. 13/2023/ND-CP and was subsequently inherited and further developed under the Law on Personal Data Protection 2025. Under Vietnamese law, personal data is defined as information in the form of symbols, writing, numbers, images, sounds, or similar forms in the electronic

[4] *Introduction to Cloud Computing*, GEEKSFORGEEKS (2026), https://www.geeksforgeeks.org/cloud-computing/cloud-computing/.

[5] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) 1, https://gdpr-info.eu/art-4-gdpr/.

 [ISSN 2581-5369]

environment that is associated with a specific person or helps to identify a specific person. Vietnamese law also classifies personal data into two categories, basic personal data and sensitive personal data, thereby applying different levels of protection to each.[6] The Law further moves closer to international standards by emphasising a data governance approach based on the accountability of data-processing entities and on the control exercised by data subjects over their personal data.

Unlike many other forms of data, personal data have not only informational value but also directly reflect personality rights protected by law. The disclosure or unauthorised use of personal data may infringe honour, dignity, reputation, personal liberty, and various other constitutionally protected rights. Importantly, rights in personal data are not extinguished when data are transferred to an organisation or enterprise. Although an enterprise may process data within the scope permitted by law or on the basis of the data subject's consent, fundamental control remains with the individual. This is a central principle of the General Data Protection Regulation and an approach that Vietnamese law is progressively adopting.

In the cloud computing environment this characteristic is particularly significant, because data are often no longer stored directly by the data subject but are entrusted to storage service providers. Without sufficiently robust legal mechanisms, individual privacy can easily be undermined by the informational and technological asymmetry between users and large technology enterprises. These approaches demonstrate that Vietnamese law has gradually moved closer to international legislative trends by broadening the scope of personal data and establishing protection mechanisms for sensitive data as well.

C. Rights and obligations of data subjects

In the context of cloud computing, personal data are often stored and processed on technological infrastructures provided by third parties and may even be transferred across multiple countries during operation. This increases the imbalance in control between individuals and data-processing organisations. Accordingly, the laws of many countries tend to expand the rights of data subjects while requiring data-processing organisations to facilitate the effective exercise of those rights, rather than merely recognising them in formal terms.

According to article 9 of the 2025 Law on Personal Data Protection, data subjects are granted a relatively comprehensive set of rights, including the right to be informed, the right to consent, the right of access, the right to rectification, the right to withdraw consent, the right to erasure, the right to restriction of processing, the right to object to data processing, the right to request

[6] Law on Personal Data Protection, No. 91/2025/QH15 (June 26, 2025) (Vietnam), art. 2, cl. 1.

 [ISSN 2581-5369]

the provision of data, the right to lodge complaints and denunciations, the right to initiate legal proceedings, and the right to claim compensation for damage where lawful rights and interests are infringed. These rights demonstrate an increasingly close alignment with international standards on personal data protection, and particularly with the General Data Protection Regulation of the European Union.

Right to be informed. This right constitutes the foundation for all other rights in the field of personal data protection. Data subjects can exercise meaningful control over their data only where they are provided with sufficient information regarding the purposes of processing, the scope of use, the retention period, the entities having access to the data, and the potential risks arising during processing. Under Vietnamese law, the processing of personal data must in principle be based on the data subject's voluntary, explicit, and verifiable consent, except where otherwise provided by law. This approach is consistent with article 6 of the General Data Protection Regulation, under which consent is valid only where it is given freely, specifically, in an informed manner, and unambiguously.

Right of access, rectification, and updating of data. This right enables individuals to ascertain what information is being collected, the purposes for which it is processed, the source of the data, and the entities to which the data have been or are being disclosed.

Right to erasure and withdrawal of consent. The right to request the erasure of personal data represents one of the significant advances in modern data protection law. Vietnam's 2025 Law on Personal Data Protection recognises the right to request erasure in various circumstances and permits data subjects to withdraw their consent at any time, unless otherwise provided by law.

Right to object. The right to object to data processing enables data subjects to request the termination or restriction of a specific processing activity, even where the processing was previously carried out lawfully. This right reflects a shift from a model of data protection toward a model of empowering individuals to control their data, and it reflects a broader trend pursued by many jurisdictions in developing and refining their personal data protection frameworks.[7]

D. Data protection principles and risks in the cloud computing environment

The development of cloud computing has created a data-processing environment that differs fundamentally from the traditional storage model. Under this architecture, data are no longer stored centrally on server systems directly controlled by an organisation; they are distributed across multiple data centres and jurisdictions and processed through the involvement of various

[7] Law on Personal Data Protection, No. 91/2025/QH15 (June 26, 2025) (Vietnam), art. 10.

 [ISSN 2581-5369]

entities. Vietnamese law has established clear principles for the protection of personal data,[8] namely:

1. compliance with the Constitution, with the Law on Personal Data Protection, and with other relevant laws and regulations;
2. that personal data may be collected and processed only within a specific and clearly defined scope and for specific and clearly stated purposes, in compliance with applicable laws and regulations;
3. ensuring the accuracy of personal data and allowing it to be corrected, updated, and supplemented where necessary, personal data being retained for a period appropriate to the purposes of processing unless otherwise provided by law;
4. effectively and consistently implementing appropriate institutional, technical, and human measures to protect personal data;
5. proactively preventing, detecting, and combating violations, and promptly and strictly addressing all violations of personal data protection law; and
6. integrating personal data protection with the protection of national interests, supporting socio-economic development, and ensuring national defence, security, and foreign relations, while striking an appropriate balance between personal data protection and the legitimate rights and interests of agencies, organisations, and individuals.

The protection of personal data is not limited to technical solutions but must also comply with a strict set of legal principles aimed at ensuring the data subject's right of self-determination over personal data.[9] However, when using cloud computing services, data subjects may face various risks to the security and integrity of their personal data. The risk of data leakage and unauthorised access is among the most common and potentially serious. In the cloud computing environment data are often stored centrally on a very large scale, which makes data centres attractive targets for cyberattack. Beyond external attacks, risks may also arise from system misconfiguration, inadequate access-control management, or the conduct of internal personnel.

A distinctive feature of cloud computing is that data may be transferred automatically between data centres located in different countries in order to optimise system performance. Another emerging trend is the integration of artificial intelligence tools and big data analytics to derive value from personal data. Although these technologies offer significant benefits in business

[8] Law on Personal Data Protection, No. 91/2025/QH15 (June 26, 2025) (Vietnam), art. 3.
[9] Dinh Xuan Cuong, *Personal Data Protection Law in Vietnam: Gaps and Directions for Improvement*, VIETNAM INTEGRATION J., No. 373 (Nov. 2025).

 [ISSN 2581-5369]

efficiency and innovation, they also increase the risk of privacy infringement through the creation of individual profiles, behavioural prediction, and automated decision-making. The foregoing analysis shows that the principles of personal data protection under Vietnamese law are, in general, increasingly aligned with international standards, particularly the principles of lawfulness, transparency, purpose limitation, and data security. In the cloud computing context, however, the challenge no longer lies in the absence of principles but in the ability to operationalise them through appropriate governance mechanisms and technologies.

III. THE CURRENT STATE OF PERSONAL DATA PROTECTION IN THE USE OF CLOUD COMPUTING SERVICES

A. Vietnamese legal regulation of personal data protection in cloud computing

The rapid development of cloud computing has fundamentally transformed the ways in which government agencies, businesses, and individuals store, manage, and use data. Whereas under traditional information technology models data were primarily stored on servers directly managed and controlled by an organisation, in the cloud computing environment data are distributed across multiple data centres, processed through various service layers, and may be transmitted across multiple countries within a very short period. These characteristics significantly increase the risks of privacy infringement, data breach, and unauthorised access, while also giving rise to new legal questions concerning the determination of regulatory jurisdiction, the responsibilities of relevant entities, and mechanisms for cross-border data protection.

At present Vietnam has not enacted a separate specialised law governing the provision and use of cloud computing services. Nevertheless, in recent years its legal framework on personal data protection has gradually been developed in alignment with international standards, establishing a multi-layered framework in which matters relating to cloud computing are regulated through various legal instruments. That framework establishes general principles for personal data protection while also imposing obligations on entities involved in data processing in the digital environment.

Article 21 of the Constitution provides that everyone has the right to inviolability of private life, personal secrets, and family secrets; that information concerning private life and personal secrets is protected by law; and that the collection, retention, use, and disclosure of information relating to an individual's private life must be consented to by that person, except where otherwise provided by law. Although this provision does not refer directly to personal data or cloud computing, it establishes a constitutional principle of individual self-determination over

 [ISSN 2581-5369]

personal information and serves as the foundation for the development of specialised regulation of data protection in the digital environment.

The 2015 Civil Code further elaborates the rights relating to private life, personal secrets, and family secrets. Article 38 provides that the collection, retention, use, and disclosure of information relating to an individual's private life must be consented to by that person, and prohibits unauthorised access to, use of, or disclosure of personal information. The Civil Code, however, approaches these matters primarily from the perspective of personality rights and does not adequately address issues specific to data processing in the digital environment, such as cross-border transfers, automated processing, or the responsibilities of cloud computing service providers.

The 2025 Law on Personal Data Protection elevated the regulation of personal data protection from the level of a governmental decree to that of a statute, thereby establishing a more stable legal foundation with greater authority. Compared with Decree No. 13/2023/ND-CP, the 2025 Law not only retains the principles governing data processing but also expands the mechanisms for protecting the rights of data subjects and further clarifies the responsibilities of data controllers, data processors, and entities that both control and process personal data. In particular, the Law adopts a clearer approach to the principle of accountability, one of the core principles of the General Data Protection Regulation. Under that principle, entities processing personal data are not only required to comply with applicable law but must also be able to demonstrate compliance through appropriate governance measures, internal controls, and the maintenance of records of data-processing activities.[10]

With respect to cloud computing, although the 2025 Law does not establish a separate chapter governing cloud services, many of its provisions have direct implications for them. Requirements concerning data-processing impact assessments, the regulation of cross-border data transfers, the protection of sensitive personal data, notification of personal data breaches, and the implementation of appropriate technical measures constitute fundamental obligations for both cloud computing service providers and the organisations that use their services.

Vietnam's current legal framework for personal data protection in the cloud computing environment has developed as a multi-sectoral and multi-layered framework, combining provisions of civil law, cybersecurity law, electronic transactions law, information technology law, and specialised personal data protection legislation. This approach broadens the regulatory scope and provides a relatively comprehensive legal basis for data processing. However,

[10] Regulation (EU) 2016/679, *supra* note 5, art. 5(2).

 [ISSN 2581-5369]

compared with jurisdictions that have enacted dedicated cloud computing legislation or issued specific technical guidance for cloud service providers, Vietnamese law still regulates cloud computing primarily through general personal data protection provisions.

B. Legal gaps and limitations

Although Vietnam's legal framework for personal data protection has made significant strides recently, the current legal landscape still contains numerous gaps and limitations regarding data governance in cloud computing environments. These stem not only from the rapid pace of technological advance but also from the disconnect between traditional legal regulation and the distributed, cross-border, multi-party data processing models characteristic of cloud computing services.

First, Vietnamese law does not yet contain dedicated provisions governing the provision and use of cloud computing services. Regulation of personal data protection in the cloud environment is scattered across various instruments, such as the 2025 Law on Personal Data Protection, the 2018 Law on Cybersecurity, the 2023 Law on Electronic Transactions, and the 2006 Law on Information Technology, together with their implementing regulations. While this establishes a relatively comprehensive legal framework for data processing in general, it does not yet fully reflect the specific characteristics of cloud computing.

Unlike traditional storage models, cloud computing operates on the basis of resource sharing among multiple customers, providers, and data centres located in different countries. In a cloud service transaction, personal data may simultaneously be processed by an infrastructure provider, a platform provider, a software provider, and multiple subcontractors. Vietnamese law, however, continues to classify actors primarily under the concepts of data controller, data processor, and controller cum processor, without specific provision on the legal status, scope of liability, or coordination mechanisms among cloud service providers within the data-processing chain.

This gap creates difficulty in determining liability when a data security incident occurs. In many cases the service user contracts only with a primary provider, while the data are actually stored or processed through several auxiliary providers. If a violation occurs, identifying the party liable for compensation or for breach notification becomes complicated by the absence of a legal basis governing relationships among actors in the service supply chain.

Second, provisions on accountability and the allocation of responsibility among actors remain largely principles-based and are not yet sufficiently adapted to the cloud computing governance model. One of the progressive aspects of the 2025 Law is its adoption of the accountability

 [ISSN 2581-5369]

principle, aligning with the direction taken by the General Data Protection Regulation.[11] The existing rules, however, primarily require entities to assume responsibility or to demonstrate compliance, without clearly defining the scope and content of accountability in the cloud computing environment. The mechanisms for exercising the rights of data subjects also lack specific provision on time limits, procedures, and responsibilities for handling requests. Although the law recognises the right to request erasure and the right to object to processing, it does not yet provide sufficiently detailed guidance on how to address backup copies, data synchronised across multiple cloud platforms, or data already shared with third parties. These gaps may undermine the effectiveness of data subjects' rights in practice. Vietnamese law does not yet specify the contents of accountability documentation, compliance assessment criteria, or periodic inspection mechanisms applicable to cloud service providers. As a result, many enterprises have focused primarily on technical measures such as encryption and access control without establishing comprehensive data governance systems.

Third, the enforcement capacity and compliance awareness of enterprises remain limited. Beyond the legal gaps, practical enforcement of personal data protection regulation remains challenging. For many Vietnamese enterprises, and particularly small and medium-sized enterprises, investment in data governance systems has not been treated as a priority. Many select cloud computing services primarily on the basis of cost, without sufficient attention to contractual provisions on data processing, data storage locations, audit rights, or liability in the event of a breach. Specialised human resources for personal data protection also remain inadequate in both quantity and quality. Many enterprises have no dedicated data protection unit and have not established data risk assessment procedures before deploying cloud computing systems. This increases the risk of legal violation.

The foregoing analysis indicates that the most significant gap in Vietnamese law no longer lies in the absence of personal data protection principles, but in the failure to establish a dedicated legal governance mechanism for cloud computing. Existing provisions regulate data processing in general, whereas cloud computing is a distributed, cross-border model dependent on a multi-tier service supply chain. Comparison with the General Data Protection Regulation shows that Vietnamese law has converged with international standards at the level of principle but still has a significant gap in enforcement instruments, including data protection impact assessments, the principle of privacy by design, the management of sub-processors, cloud service certification, independent audit, and international data-transfer mechanisms. All of these are critical to the effective protection of personal data in the digital economy.

[11] Regulation (EU) 2016/679, *supra* note 5.

 [ISSN 2581-5369]

IV. RECOMMENDATIONS

The analysis of the current legal landscape and of the gaps in personal data protection mechanisms within cloud computing environments shows that the present imperative extends beyond merely refining legal regulation. It also requires the establishment of a modern data governance framework tailored to the specific characteristics of cloud computing models and to the development trends of the digital economy.

First, a dedicated legal framework should be developed governing the provision and use of cloud computing services. The experience of the European Union shows that, although the General Data Protection Regulation does not enact a separate cloud computing law, its clear allocation of responsibility among data controllers, data processors, and sub-processors, together with guidance from the European Data Protection Board, has established a relatively comprehensive governance mechanism for data processing on cloud platforms. That is an experience on which Vietnam may draw.

Although the 2025 Law on Personal Data Protection has established an important foundation, its provisions still regulate data processing in general and do not fully reflect the specific characteristics of cloud computing. Vietnam should therefore consider developing a dedicated legal framework for cloud computing services, potentially in the form of a Government decree or a specialised circular providing guidance on data governance and protection in the cloud environment. Such an instrument should regulate the cloud service models clearly and determine the legal status of each actor in the service supply chain, including infrastructure providers, platform providers, software providers, and auxiliary providers. It should also clarify the scope of liability, the obligations of coordination, and the mechanisms for allocating liability among actors when data security incidents occur, so as to avoid the present overlap and gaps in responsibility.

Second, accountability and data governance mechanisms should be specified on a risk-based approach. One of the major gaps in current Vietnamese law is that the accountability principle remains broadly formulated. Provisions concerning the content, methods, and criteria for implementing accountability by organisations processing data on cloud platforms should therefore be developed further. The law should require data-processing organisations to establish data governance documentation, maintain data-processing logs, conduct data protection impact assessments for high-risk processing activities, and develop procedures for responding to data breaches. It is also necessary to stipulate clearly the timeframes and

 [ISSN 2581-5369]

procedures for addressing requests from data subjects concerning rights such as erasure, withdrawal of consent, or objection to processing.

Third, certification and independent audit mechanisms should be established for cloud computing services. To enhance transparency and the verifiability of legal compliance, Vietnam should consider establishing a data security certification mechanism for cloud service providers based on international standards such as ISO/IEC 27017, ISO/IEC 27018, and ISO/IEC 27701, or on the certification framework of the Cloud Security Alliance.[12] Periodic audit requirements should also be introduced for enterprises processing large volumes of personal data or providing cloud computing services to State agencies and to sensitive sectors such as finance, banking, healthcare, and education. Audit results should serve as a basis for assessing legal compliance while enabling service users to select providers that meet data protection standards.

Fourth, the mechanism regulating cross-border transfers of personal data should be improved. Given the global development of cloud computing, cross-border data flows should be governed in a manner that both safeguards data sovereignty and facilitates digital investment and trade. In addition to the existing administrative mechanisms, Vietnam should consider introducing flexible legal instruments similar to those under the General Data Protection Regulation, such as standard contractual clauses, binding corporate rules, or mechanisms recognising an adequate level of data protection in certain countries or territories. Diversifying transfer mechanisms would help reduce compliance costs for enterprises while maintaining an appropriate level of personal data protection.

Fifth, law-enforcement capacity and the compliance awareness of enterprises should be strengthened. Beyond improving the legal framework, the effectiveness of personal data protection depends heavily on the enforcement capacity of the actors involved in data processing. Guidance, training, and support for enterprises, and particularly for small and medium-sized enterprises, should be strengthened to assist them in establishing data governance systems consistent with legal requirements. State management agencies should issue technical guidance on data risk assessment, cloud service contract management, service-provider selection, and data breach incident response, and enterprises should be encouraged to establish dedicated data protection units or to appoint data protection officers where they process large volumes of personal data. International cooperation in human-resource training, the sharing of data governance experience, and participation in regional personal data protection initiatives

[12] INT'L ORG. FOR STANDARDIZATION, *ISO/IEC 27017:2015, Information Technology, Security Techniques, Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services* (2015).

 [ISSN 2581-5369]

should also be strengthened, so as to enhance Vietnam's enforcement capacity in the context of digital integration.

V. Conclusion

Improving the mechanism for protecting personal data in the use of cloud computing services should proceed in a coordinated manner through legal reform, innovation in governance approaches, and enhanced enforcement capacity. The focus should not only be on adding new rules but also on building a risk-based, transparent, and accountable data governance model consistent with the characteristics of cloud computing and with international standards. This will provide an important foundation for safeguarding individual privacy, strengthening digital trust, and promoting sustainable digital transformation in Vietnam.

*****

 [ISSN 2581-5369]