



Working Paper 2026
- Vol. 2, No. 2

CHÍNH SÁCH BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA SINGAPORE CHO KHÁCH HÀNG MUA SẴM TRÊN CÁC SÀN THƯƠNG MẠI ĐIỆN TỬ: HÀM Ý CHÍNH SÁCH CHO VIỆT NAM

Nguyễn Hoàng Anh Thư¹, Đỗ Thị Thùy Lan, Nguyễn Thị Thu Hà,
Nguyễn Minh Anh Đào, Võ Như Quỳnh

Sinh viên K63 CLC Quản trị kinh doanh quốc tế - Khoa Quản trị kinh doanh & Tài chính
- Kế toán

Phân hiệu Trường Đại học Ngoại Thương tại Thành phố Hồ Chí Minh, Việt Nam

T.S Thái Văn Thơ

Giảng viên Bộ môn Khoa học Cơ bản

Phân hiệu Trường Đại học Ngoại Thương tại Thành phố Hồ Chí Minh, Việt Nam

Tóm tắt

Sự mở rộng nhanh chóng của thương mại điện tử - “E-commerce” trong thúc đẩy tăng trưởng kinh tế số đã làm gia tăng lo ngại về việc bảo vệ dữ liệu cá nhân của khách hàng mua sắm trên các sàn thương mại điện tử phụ thuộc vào việc thu thập và xử lý dữ liệu quy mô lớn. Nghiên cứu tập trung phân tích khuôn khổ chính sách của Singapore về bảo vệ dữ liệu cá nhân khách hàng trên các nền tảng thương mại điện tử, đặc biệt chú trọng vào khai thác Đạo luật Bảo vệ Dữ liệu Cá nhân (PDPA). Thông qua phương pháp nghiên cứu so sánh kết hợp tiếp cận quy phạm, pháp luật xã hội học và thực nghiệm, bài viết đánh giá mô hình quản trị dữ liệu của Singapore với cấu trúc quản trị tập trung và thích ứng đã đảm bảo tính thống nhất quy định, trách nhiệm giải trình của doanh nghiệp, và lòng tin công chúng, định vị quốc gia dẫn đầu trong khu vực Đông Nam Á. Từ đó, nhận diện những khoảng trống chính sách của Việt Nam và đề xuất các khuyến nghị nhằm tăng cường năng lực thực thi, quản trị dữ liệu xuyên biên giới.

Từ khoá: Chính sách bảo vệ dữ liệu, quản trị dữ liệu, E-commerce, quyền riêng tư người dùng, bài học từ Singapore.

¹ Tác giả liên hệ, Email: k63.2412255061@ftu.edu.vn

POLICY ON PROTECTING CUSTOMERS' PERSONAL DATA ON E-COMMERCE PLATFORMS IN SINGAPORE: RECOMMENDATIONS FOR VIETNAM

Abstract

The rapid expansion of E-commerce in growing the digital economy has intensified concerns about the protection of customers' personal data, as online platforms rely heavily on large-scale data collection and processing. This study examines Singapore's policy framework for protecting personal data on e-commerce platforms, focusing on the *Personal Data Protection Act (PDPA)*. Using a comparative research approach that integrates normative, socio-legal, and empirical methods, the paper evaluates Singapore's data governance model across three key institutional dimensions: structural framework, governance capacity, and compliance culture. Findings reveal that Singapore's centralized and adaptive governance structure ensures regulatory coherence, corporate accountability, and public trust positioning it as a regional leader in Southeast Asia. The paper identifies policy gaps in Vietnam's framework and proposes actionable recommendations for enhancing enforcement, cross-border data governance.

Keywords: Data protection policy, data governance, E-commerce, consumer privacy, Singapore experience.

1. Introduction

1.1. Definition of the Concepts related to the Study

Data Protection Policy

The concept of data protection policy in Singapore reflects a balanced approach between safeguarding individual privacy and enabling legitimate business activities. Under the Personal Data Protection Act (PDPA), Singapore recognizes both the right to personal data privacy and the need for organizations to collect, use, and disclose data for reasonable purposes. The policy establishes a comprehensive data protection regime, ensuring that personal data is not misused and that individuals maintain confidence in e-commerce platforms and online service providers.

From a semantic perspective, key terms such as privacy, trust, transparency, and legitimacy are central to understanding Singapore's approach. Privacy denotes the consumer's right to control and consent regarding personal data collection and use. Trust represents the outcome of effective data protection, reinforcing long-term consumer–business relationships. Transparency refers to firms' obligation to clearly communicate data practices, while legitimacy underscores the ethical and lawful purposes behind data usage.

For Vietnam, this interpretation offers crucial lessons that were emphasized by To Lam the Minister of Public Security, “protecting personal data has become an urgent and practical issue amid the country's rapid digital transformation” (Government Electronic Newspaper, 2023). Vietnam can learn from Singapore's model by developing a framework that balances consumer rights and business innovation, embedding ethical principles of fairness, trust, and transparency into national e-commerce policies. This would not only enhance consumer confidence but also strengthen Vietnam's competitiveness in the regional digital economy.

Data Governance

Data governance refers to the exercise of authority, control, and shared decision-making over the management of data assets within an organization (Brous, Janssen and Vilminko-Heikkinen, 2016). It ensures that data is collected, processed, and used appropriately, providing the right people with the right information at the right time. From a conceptual standpoint, data governance operates across multiple dimensions from technological, managerial, cognitive, and comprehensive emphasizing both the strategic value of data and the mechanisms that safeguard its quality, consistency, and security. Semantically, it integrates elements of accountability, standardization, and transparency, positioning data as an enterprise asset that requires coordinated policies, standards, and responsibilities to maximize value and support informed decision-making.

E-commerce

The concept of E-commerce refers specifically to digital platforms such as Shopee, Lazada, and TikTok Shop online marketplaces that “build bilateral or multilateral trading environments through modern information technology to facilitate commercial activities for profit” (Li, 2023). These E-commerce platforms operate as intermediaries connecting sellers and consumers, while simultaneously functioning as data-driven enterprises that collect, store, and analyze vast amounts of user and transaction data (Li, 2024). Legally, personal data is defined as information identifying or helping to identify specific individuals, including both basic and sensitive types; once identified, it is no longer classified as personal data (Law on Personal Data Protection 2025 No 91/2025/QH15 in Vietnam, n.d.). Thus, E-commerce platforms are not only online marketplaces but also complex digital ecosystems that necessitate robust mechanisms for data privacy and consumer protection.

Privacy

Consumer privacy refers to an individual’s right and ability to control, understand, and consent to the collection and use of personal information in marketing activities. It includes both the control of access to one’s personal and transactional data and the awareness of how firms collect, process, and disclose such data (Goodwin 1991; Foxman and Kilcoyne 1993; Nowak and Phelps 1995; Lanier and Saini 2008). Privacy concerns arise when consumers perceive that their information is improperly collected, monitored, stored, or transferred without consent, leading to potential misuse or unauthorized disclosure (Wang, Lee and Wang 1998). Because privacy expectations vary across individuals, situations, and cultures, consumer privacy is not absolute and often involves ethical considerations of fairness, trust, and transparency between consumers and firms (Milne and Gordon, 1993).

1.2. Theoretical Framework

To systematically evaluate the effectiveness of data protection regimes in Singapore and Vietnam, this study constructs a multi-dimensional governance framework synthesized from international best practices. Moving beyond a superficial comparison of legal statutes, the analysis

posits that successful policy implementation relies on the interplay of three core pillars: Institutional Structure, Governance Capacity, and Compliance Culture. This approach ensures a holistic assessment of how data privacy regulations function in practice rather than just in theory.

Initially, institutional structure draws upon the guidelines established by the OECD (2021) to assess the regulatory architecture. This pillar focuses specifically on the legal autonomy and design of supervisory authorities. It argues that for a data protection regime to be credible, the regulator must possess sufficient independence to exercise oversight without undue political or commercial interference.

Building on this structural foundation, the second dimension examines governance capacity. Guided by the criteria outlined by UNCTAD (2016) for developing digital economies, this section evaluates the tangible resources available for enforcement. It scrutinizes whether the regulatory bodies in Singapore and Vietnam possess the necessary administrative power, technical capabilities, and financial resources to translate legal mandates into effective execution.

Finally, the framework incorporates compliance culture as the third dimension. Grounded in the indicators defined by the World Bank (2021), this pillar analyzes the maturity of the market and society. It assesses the extent to which businesses voluntarily adopt privacy measures and the level of public trust in the digital ecosystem, viewing these factors as the ultimate validation of a regulatory regime's success.

2. Research Methods

This study adopts a qualitative research design that integrates multiple complementary approaches namely comparative analysis, argumentative reasoning, logical method, historical methodology, and the theoretical lens of critical realism to examine the governance and protection of consumers' personal data on e-commerce platforms in Singapore and Vietnam. The multi-method framework enables a comprehensive understanding of both the structural and contextual dimensions that shape data protection policies within digital economies.

The comparative and analytical approach is utilized to identify the strengths, weaknesses, and distinctive features of Singapore's data protection framework, particularly its *Personal Data Protection Act (PDPA)* and enforcement under the unique authorized *Personal Data Protection Commission (PDPC)* to draw applicable lessons for Vietnam. By systematically comparing institutional structures, governance capacity, and compliance culture, the research evaluates how each country's regulatory system affects the protection of consumers' personal data in e-commerce environments. This method enables the identification of policy gaps, best practices, and the potential for policy transfer between the two jurisdictions.

Complementing this, the critical realism approach is applied to uncover the underlying causal mechanisms behind both the successes and constraints in Vietnam's policy implementation. Rather than focusing solely on legal provisions, this framework explores the deeper structural issues within institutional design, administrative efficiency, and behavioral compliance that influence data

protection outcomes. Through this lens, the study seeks to generate evidence-based recommendations tailored to Vietnam's digital data governance landscape.

3. Policy on Protecting Customers' Personal Data on E-commerce Platforms in Singapore

3.1. Overview

Singapore's e-commerce environment is governed by a comprehensive legal and institutional framework designed to promote innovation, consumer trust, and cybersecurity. Key regulatory authorities include the Accounting and Corporate Regulatory Authority (ACRA), the Infocomm Media Development Authority (IMDA), and the Personal Data Protection Commission (PDPC). Together, these agencies ensure that online businesses comply with corporate, data protection, and digital communication standards.

ACRA oversees corporate registration and compliance under the Companies Act, ensuring that e-commerce enterprises operate transparently and within legal boundaries. Meanwhile, IMDA plays a dual role: it promotes digital transformation and enforces data governance regulations through the PDPC (Yoonhee Jeong, 2023).

3.2. Policy Framework on Personal Data Protection in Singapore

Singapore has effectively established a sophisticated policy framework for the protection of personal data, positioning itself as a reliable global hub for the digital economy. Through three strategic dimensions: a centralized institutional structure, comprehensive governance capacity, and a compliance-oriented culture, this framework actively promotes a secure e-commerce ecosystem rather than merely regulating it.

3.2.1. Institutional structures

Singapore's agile and unified institutional structure, which successfully removes regulatory fragmentation, is the key to its successful digital governance. The Info-communications Media Development Authority Act of 2016 established Singapore's "umbrella" governance model, which differs from other jurisdictions' fragmented models. This Act, which was passed on August 22, 2016, and went into effect on October 1, 2016, incorporated the Personal Data Protection Commission (PDPC) into the Info-communications Media Development Authority (IMDA). The PDPC functions as a statutory office under this arrangement, guaranteeing that data protection regulations are in line with the larger objectives of the media and technology industries rather than acting as stand-alone obstacles. By facilitating a coordinated approach where all personal data issues are handled by a single authority, this integration improves regulatory consistency and fosters collaboration between media and data protection policies.

The institutional structure incorporates a strong check-and-balance mechanism through the Data Protection Appeal Panel (DPAP) to guarantee that this centralized power is used fairly and responsibly. The DPAP, which is governed by the Personal Data Protection (Appeal) Regulations 2021, offers individuals and organizations an impartial and open way to examine PDPC

enforcement decisions. Businesses have 28 days to file an appeal about instructions or fines. This mechanism lowers perceived legal risks for foreign investors and digital platforms investing in Singapore by ensuring that the regulatory environment remains objective.

3.2.2. Governance capacity

A comprehensive legal toolkit that blends fundamental privacy laws with market-driven mechanisms and supporting digital legislation sets Singapore apart in terms of its governance capacity. The Personal Data Protection Act 2012 (PDPA), which was passed by Parliament in October 2012 and went into full effect on July 2, 2014, is the cornerstone of this capacity. For the protection of personal data on both traditional and electronic platforms, the PDPA sets a baseline standard. It ensures that e-commerce platforms handle customer information responsibly by imposing crucial obligations on organizations, such as consent, purpose limitation, accuracy, and retention. In particular, businesses must only gather data with permission, use it for legitimate purposes, and protect it with the proper security measures.

The Do Not Call (DNC) Registry is a crucial part of the PDPA that improves consumer control. People can choose not to receive unsolicited marketing calls and messages by using this national registry. Before sending any marketing communications, organizations must rigorously compare their contact lists to the DNC database using a DNC Check within 30 days. The PDPC has the authority to impose financial penalties on a company that does not comply. This mechanism increases public trust by compelling e-commerce companies to switch from spam-based marketing to consent-based tactics. The Data Protection Trustmark (DPTM) certification scheme, a voluntary standard that enables compliant platforms to display a seal of trust, helps consumers differentiate trustworthy sellers from dishonest ones, and lessens information asymmetry in the online market.

A number of complementary digital laws that establish a safe harbor for digital trade strengthen Singapore's governance capacity in addition to the fundamental data protection laws. Digital contracts are just as legitimate as physical ones thanks to the Electronic Transactions Act of 2010, which supports the legal recognition of electronic records and signatures. This gives safe online payment and authentication systems the legal basis they need. Additionally, the Foreign Interference (Countermeasures) Act 2021 (FICA) and the Protection from Online Falsehoods and Manipulation Act 2019 (POFMA) safeguard the digital sphere. FICA deals with threats from foreign actors, while POFMA gives authorities the authority to rectify false information. By preventing the manipulation of the information environment in which e-commerce takes place, these laws collectively guarantee the integrity and security of the digital economy.

3.2.3. Compliance culture

Lastly, Singapore has developed a compliance culture that emphasizes substantive accountability while striking a balance between stringent enforcement and remedial flexibility. The Personal Data Protection (Enforcement) Regulations 2021 established comprehensive investigative protocols, giving the PDPC the authority to demand the production of documents, question witnesses, and issue enforcement directives. These instructions may include ordering a company

to cease data processing or fixing incorrect data. Crucially, enforcement outcomes are made public, improving transparency and assisting consumers in selecting reliable online platforms.

However, the framework takes a practical approach through the Personal Data Protection (Composition of Offences) Regulations 2021, acknowledging that complete security is difficult in this fast-paced digital economy. The Commission may compound minor offenses under these regulations, giving remedial outcomes precedence over prosecution. Instead of dealing with drawn-out legal procedures, this strategy encourages e-commerce sellers to concentrate resources on improving internal systems and implementing corrective measures. Strict transparency requirements under the Personal Data Protection (Notification of Data Breaches) Regulations 2021 balance this flexibility. After identifying a major breach, organizations have three calendar days to notify the PDPC and the impacted parties. This required disclosure guarantees that accountability for e-commerce platforms handling sensitive payment data is non-negotiable and enables users to take preventative action quickly, preserving long-term trust in the digital sector.

3.3. Achievement

The implementation of the Personal Data Protection Act (PDPA) in 2012 has established Singapore as an adaptive data governance model in the region with the foremost achievement being the establishment of a baseline data protection standard for the private sector, which strengthens public trust and fosters robust corporate accountability.

3.4.1. Fortifying economic with trust

The PDPA has solidified Singapore's status as a trusted global data hub. This legal framework facilitates the signing of Digital Economy Agreements (DEAs), enabling secure cross-border data flows and thereby contributing to national prosperity by sustaining capital and data movement. This regulatory harmonization enhances the international interoperability of Singaporean enterprises, supporting their expansion in the globalized e-commerce market. The successful enforcement structure ensures regulatory coherence across all sectors (Wong, 2017).

3.4.2. Consumer protection

From a societal perspective, the PDPA has substantially increased individual data autonomy. The introduction of the Do Not Call (DNC) Registry is a significant empirical tool that grants individuals direct control over unwanted marketing communications, which demonstrably improves quality of life and promotes an ethical compliance culture in commercial activities (PDPC, 2021). Specifically for online transactions, the PDPA mandates explicit consent and mandatory security obligations on e-commerce platforms, ensuring a more transparent and secure environment for customers.

3.4.3. Market dynamics and institutional challenges

The PDPA has stimulated the growth of high-quality employment by creating demand for specialized roles such as Data Protection Officers (DPOs) and bespoke compliance services (Zee Kin, 2022). However, this model faces the practical challenge of compliance costs which can be burdensome for Small and Medium Enterprises (SMEs). Furthermore, sustaining the regulatory

balance between protecting privacy rights and enabling data-driven innovation remains a continuous tension, necessitating frequent guidance and intervention from the Personal Data Protection Commission (PDPC) to ensure consistent and effective enforcement (PDPC, 2021).

a. Positive achievements and socio-economic implications

The PDPA's core achievement is the creation of a baseline data protection standard for the private sector, founded on principles such as consent, purpose limitation, and mandatory security. This framework has significantly bolstered public trust and enhanced corporate accountability critical non-market factors sustaining the growth of e-commerce and the broader digital economy.

In terms of global positioning, the PDPA has been instrumental in establishing Singapore as a trusted global data hub (PDPC, 2022). Its regulatory alignment with international norms (like the GDPR) facilitates the negotiation of Digital Economy Agreements (DEAs), enabling secure cross-border data flows with key partners (e.g., the EU, New Zealand, Chile). This institutional architecture directly supports national prosperity by maintaining the flow of capital and data, thereby sharpening the competitive advantage of Singaporean enterprises. Furthermore, the innovative Do Not Call (DNC) Registry mechanism empowers consumers with data autonomy over direct marketing, promoting an ethical compliance culture within the e-commerce sector and improving the quality of life by reducing unsolicited contact (PDPC, 2021). The PDPA also stimulated job creation in the digital governance sector, fostering high-quality employment roles, such as Data Protection Officers (DPOs), and encouraging responsible innovation within a defined legal perimeter.

b. Challenges and regulatory tensions

Despite its successes, the PDPA model presents certain challenges. Primarily, compliance costs remain a notable burden for Small and Medium Enterprises (SMEs), requiring substantial investment in technology and internal process development to meet security and breach notification obligations. Furthermore, the inherent regulatory tension between privacy protection and enabling data-driven business models necessitates constant, agile updating of guidance by the PDPC (PDPC, 2022). A historical structural limitation was the PDPA's initial exclusion of public sector agencies, creating a fragmented approach to data accountability across state and non-state actors, though this gap has since been addressed by subsequent public sector regulations.

c. Reinforced E-commerce consumer rights

Crucially for online consumers, the PDPA reinforces several key rights on e-commerce platforms: Active Consent is mandatory for data collection and disclosure; enterprises bear a Mandatory Security Obligation to protect user data; the DNC Registry offers a simple Opt-Out Mechanism against unwanted promotions; and the Mandatory Data Breach Notification duty ensures timely transparency, empowering consumers to mitigate potential harm (DLA Piper, 2024).

4. Policy Recommendations for Vietnam

4.1. Policy Framework on Personal Data Protection in Vietnam

First of all, Vietnam's institutional architecture for personal data protection has undergone a significant transformation from a decentralized, sector-specific model to a highly centralized framework. Historically, enforcement was fragmented across various laws such as the Law on Information Technology 2006, which laid the initial foundation for privacy in cyberspace (Vietnam National Assembly, 2006), and the Civil Code 2015, which recognized personal information as a civil right (Vietnam National Assembly, 2015). However, these regulations lacked a specialized enforcement agency. The trajectory changed with the Cyber Security Law 2018, which introduced data localization requirements and assigned oversight to the Ministry of Public Security (Vietnam National Assembly, 2018). This centralization was solidified by Decree 13/2023/ND-CP, which designated the Department of Cyber Security and High-Tech Crime Prevention (A05) under the Ministry of Public Security as the focal agency responsible for enforcement (MPS, 2023). Most recently, the upcoming Law on Personal Data Protection (Law No. 91/2025/QH15) is expected to upgrade this authority from a decree level to a national law, aiming to harmonize regulations and strengthen enforcement powers effective from 2026 (MPS, 2025).

In terms of governance capacity, Vietnam currently does not have an independent agency specializing in personal data protection; the right to manage and enforce is assigned to many different state agencies, of which the Ministry of Public Security plays a core role. Specifically, Article 29 of Decree 13/2023/ND-CP stipulates that the professional agency for personal data protection is the Department of Cyber Security and High-Tech Crime Prevention - Ministry of Public Security, responsible for assisting the Ministry of Public Security in performing the state management of personal data protection (Cao Ky, 2023). Besides, the personal data protection force also includes: personal data protection departments and personnel in agencies and organizations; organizations and individuals providing personal data protection services; organizations and individuals mobilized to participate in protecting personal data (Hoang Ngoc, 2025). In general, there is no single specific agency with comprehensive responsibility for personal data protection. Moreover, the resources and sanctions currently positioned by the Vietnam governance capacity to enforce the law on personal data protection are still limited. While Article 4 of Decree 13/2023/ND-CP clearly states that agencies, organizations, and individuals committing violations of regulations on personal data protection, depending on the severity of the violation, may be subject to disciplinary actions, administrative sanctions, and criminal prosecution under regulations, as of the end of 2023, there has not been a separate decree on administrative sanctions for acts of infringement on personal data protection (Kim Thanh, 2023).

Finally, the development of a compliance culture for personal data protection in Vietnam is becoming more feasible as the legal framework becomes clearer. Decree 13/2023 sets out clear duties for data controllers, data processors and related actors and defines how personal data must be processed, protected and reported when violations occur. Research also shows that this shift has shaped how data privacy is interpreted in Vietnam (Huynh, 2025). The Ministry of Public

Security plays the central role in guiding and monitoring compliance through technical standards, the national portal and enforcement supervision (Data Security, 2025). Even with this foundation, many organizations are still in the early stage and face issues in technical capacity, internal procedures and staff skills. Studies note that businesses need practical tools such as encryption, access control and risk assessment to improve their practices (Han, 2024; Trang, 2023). Research also indicates that public understanding of personal and sensitive data remains uneven, which limits consistent compliance in daily operations (Huynh, 2025). Survey results confirm these challenges as 43.47% of organizations do not have dedicated data protection staff and 19.45% struggle to meet PDPD requirements (Data Security, 2025). Vietnam is now preparing for the Personal Data Protection Law that will take effect in 2026, which will increase legal obligations and strengthen enforcement and therefore create stronger pressure for organizations to build genuine compliance practices (Nguyen & Vu, 2025).

4.2. Comparisons on Policy Framework of Personal Data Protection between Singapore and Vietnam

Firstly, in terms of institutional structures, both Vietnam and Singapore demonstrate a strong convergence in their approach toward centralized governance to overcome the inefficiencies of regulatory fragmentation. As seen in Vietnam's evolution from the 2006 Law on Information Technology to the 2025 Law on Personal Data Protection, and Singapore's consolidation under the Info-communications Media Development Authority Act 2016, both nations have moved away from loose management to establish unified authorities. Furthermore, both jurisdictions rely on a state-led enforcement model where the government plays a decisive role in setting standards, rather than relying solely on industry self-regulation. In spite of the shared trend toward centralization, a fundamental difference lies in the nature of the supervisory authorities. Singapore's Personal Data Protection Commission (PDPC) operates as a statutory board within the Info-communications Media Development Authority (IMDA), aligning data protection with media convergence and economic goals. In contrast, Vietnam's enforcement acts through the Ministry of Public Security (MPS), specifically the A05 department (MPS, 2023), placing the institutional focus heavily on national security and crime prevention. Additionally, Singapore employs a structural check-and-balance mechanism through the Data Protection Appeal Panel (DPAP) governed by the Personal Data Protection (Appeal) Regulations 2021, whereas Vietnam's current framework under Decree 13 and the upcoming Law No. 91/2025 focuses primarily on inspection by the MPS without an explicit, separate administrative appeal tribunal mentioned in the primary texts (MPS, 2025).

Secondly, with regard to governance capacity, Vietnam and Singapore have some important similarities in the way they develop and implement personal data protection policies. In particular, both countries have established a dedicated state agency with the responsibility of directing, issuing guidelines and implementing tasks related to data protection. The general governance capacity of Vietnam and Singapore is based on a strong coordinating role of the State, a supportive approach to businesses and a common goal to increase consumer confidence in the digital market. In contrast,

in Singapore, the Personal Data Protection Commission (PDPC) operates as an independent body that oversees all aspects of data protection. The PDPC has clear powers to investigate, impose fines, publish enforcement decisions and provide appeal channels through the Data Protection Appeals Panel (DPAP) (PDPC, 2021). This centralized structure reflects a harmonious "umbrella" model, ensuring consistency and efficiency across sectors. In contrast, in Vietnam, the enforcement agency mainly belongs to the Ministry of Public Security (MPS), specifically the Department of Cyber Security and High-Tech Crime Prevention (A05). Although Decree 13/2023 introduced the first set of unified data protection rules, Vietnam still lacks an independent, specialized agency equivalent to the PDPC (MPS, 2023). This structural difference leads to some practical challenges. On the one hand, centralizing responsibility within the Ministry of Public Security ensures strong law enforcement capacity and cybersecurity expertise. On the other hand, it can create institutional overlap and limit transparency, as the same ministry acts as both the regulator and the enforcement agency. Therefore, businesses may face uncertainty about compliance processes, while consumers may have fewer channels of access to complain or resolve disputes.

Lastly, both Singapore and Vietnam recognize that building a compliance culture is essential for effective personal data protection. Each jurisdiction emphasizes accountability as a core principle and requires organizations to adopt internal measures that reduce risks and strengthen consumer trust. Both legal frameworks also highlight the need for timely reporting of data breaches, which encourages firms to maintain readiness and respond quickly when incidents occur. This shared focus on accountability and transparency shows that both countries view compliance as a continuous process rather than a one-time legal obligation. However, despite these similarities, the way compliance culture is shaped in each country differs significantly. Singapore promotes a proactive culture that encourages organizations to self-report and correct issues. The PDPC can compound minor offenses, which reduces fear of punishment and motivates firms to disclose incidents early. This creates an environment where compliance is linked to accountability and corrective action. By contrast, Vietnam's compliance culture is still developing. Although Decree 13 and the upcoming law provide clear duties, many organizations face challenges in technical capacity and internal readiness. Survey data shows that a large share of businesses lack dedicated staff for personal data protection, which reduces the ability to build stable compliance practices. Another difference lies in institutional structures. Singapore's enforcement is carried out by an independent authority, while Vietnam relies mainly on the Ministry of Public Security. This affects how guidance is delivered and how organizations perceive compliance obligations. Overall, Singapore operates within a mature accountability model, while Vietnam is in a transitional stage where compliance culture is still being formed and strengthened.

4.3. Recommendations for Vietnam

4.3.1. Improving institutional structures

a. Recommendation

To enhance the efficacy and fairness of its institutional framework, Vietnam should consider establishing an independent administrative appeal body similar to Singapore's Data Protection Appeal Panel. Such a body would review enforcement decisions made by the Ministry of Public Security to ensure objectivity and provide a transparent recourse for businesses. Furthermore, while maintaining necessary security protocols, the institutional authority should enhance coordination with economic ministries, such as the Ministry of Industry and Trade. This approach mirrors Singapore's integration of the PDPC within the IMDA, ensuring that data protection policies actively support the growth of the digital economy and e-commerce rather than functioning solely as security compliance measures. In addition, the growth of cross-border e-commerce has broken down national barriers, promoting borderless trade and making vital contributions to the world economy. Therefore, creating safe legal frameworks and a conducive environment is essential to promote production and trade exchange across regions (Thu Phuong, 2022). To align with these global data flows, Vietnam needs to professionalize its institutional structure to ensure a swift response to cross-border cybersecurity threats. Specifically, it requires clear jurisdiction and close coordination between e-commerce regulators and cybersecurity authorities to effectively control the collection and processing of user data from foreign platforms.

b. Potential constraints and opportunities during the implementation of Singapore's lessons in Vietnam

The implementation of Singapore's institutional lessons in Vietnam faces distinct constraints rooted in the fundamental differences between the two nations' political and administrative traditions. Unlike the commercially driven governance model of Singapore, Vietnam approaches data protection primarily through the lens of cyber sovereignty and national security, a perspective that has been deeply entrenched since the enactment of the Law on Cyber Security (Vietnam National Assembly, 2018). This security-centric focus implies that data governance is viewed as a critical component of national stability rather than merely an economic enabler, making it challenging to shift oversight functions away from the security apparatus toward a more independent or civilian-led administrative body. However, the enactment of the new Law on Personal Data Protection (Law No. 91/2025/QH15) presents a transformative opportunity to bridge this gap. This legislative milestone provides the necessary legal mandate to elevate the data protection regime from a sub-law government decree to a comprehensive national statute (MPS, 2025). This transition offers a critical window to institutionalize sophisticated governance mechanisms, such as a transparent appeal process. By embedding these checks and balances within the new law, Vietnam can harmonize its regulatory environment with international standards, thereby significantly boosting foreign investor confidence in its evolving digital economy.

4.3.2. Enhancing governance capacity

a. Recommendation

To improve the clarity in governance capacity, Vietnam should establish an independent authority dedicated to protecting personal data, similar to Singapore's Personal Data Protection Commission (PDPC). Such an agency would operate separately from law enforcement agencies,

focusing on compliance, guidance and public education rather than punishment. This agency needs to be strengthened in terms of organization, human resources, and authority to implement and monitor compliance with the law independently and transparently. At the same time, the specialized agency must closely coordinate with the relevant ministries and branches to avoid overlapping functions; clearly assigning tasks among agencies involved in personal data protection will help enhance administrative effectiveness and law enforcement efficiency. Applying a similar approach in Vietnam would reduce institutional overlap and provide a clear, accessible channel for resolving complaints and grievances.

b. Potential constraints and opportunities during the implementation of Singapore's lessons in Vietnam

One of the biggest barriers to the establishment of an independent Administrative Appeals Council in Vietnam is the lack of human resources and expertise. The effective operation of such a body requires a team of data and other interdisciplinary experts. However, in reality, according to the World Bank (WB), the supply of highly skilled human resources in Vietnam is currently very limited (Cao Tan, 2024), especially in the public sector, where it is often difficult to attract and retain high-quality experts. Therefore, if an appeals council is established without a systematic investment strategy in training, attracting and developing human resources, the risk is that the agency will operate formally, without professional capacity for making independent, objective, and effective decisions. Apart from reducing transparency and fairness in the process of law enforcement, such a situation may reduce the trust of businesses and citizens in the personal data protection mechanism.

4.3.3. Establishing compliance culture

a. Recommendation

Vietnam can strengthen its compliance culture by adapting Singapore's approach, starting with short-term actions and moving toward long-term sustainability. In practice, Vietnamese businesses are not yet fully prepared for consistent compliance, as many firms still lack technical capacity and clear internal procedures (Han, 2024; Trang, 2023). Therefore, in the short term to 2030, the government should encourage organizations to self-report minor violations to build trust and support continuous improvement (PDPC, 2021). Practical guidance, standard templates, and simple tools such as encryption, access control, and risk-assessment checklists should also be provided to help firms comply more effectively. Incentives for voluntary reporting or proactive risk management can further support the shift toward viewing compliance as a daily practice rather than only a legal formality. In the long term to 2050 and beyond, Vietnam should aim to embed compliance deeply into business culture in a sustainable manner. This includes ongoing training, sector-based support, and alignment of data protection with corporate governance standards. Gradually, legal requirements can evolve into shared norms of responsibility, supporting a mature and self-sustaining compliance environment as Vietnam moves toward full implementation of the Personal Data Protection Law (Nguyen & Vu, 2025).

b. Potential constraints and opportunities during the implementation of Singapore's lessons in Vietnam

A major constraint is Vietnam's institutional structure. Enforcement is centralized under the Ministry of Public Security, which may make firms see compliance as punishment rather than guidance (Data Security, 2025). Internal capacity is also low, with 43.47% of organizations lacking dedicated data protection staff and 19.45% unable to fully meet PDPD requirements (Data Security, 2025). These factors could slow the adoption of proactive reporting and risk-based practices. However, opportunities exist. The upcoming law and increasing public awareness of personal data rights provide a window to reshape organizational behavior (Huynh, 2025). Vietnam can adapt Singapore's lessons by emphasizing guidance, training, and incentives rather than penalties. For example, combining technical support with clear reporting procedures can help organizations implement compliance gradually. In our view, prioritizing practical support and incentives is more effective than focusing solely on enforcement. This approach can build a stable, sustainable compliance culture while avoiding excessive fear of penalties, which aligns with Vietnam's current organizational capacity and legal development stage.

5. Conclusion

This study analyzed Singapore's overall development for E-commerce data protection policy with the cornerstone of its data governance, using a three-pillar framework. The findings highlight Singapore's success through its centralized and agile institutional structure (PDPC integrated into IMDA), comprehensive governance capacity (PDPA, DNC Registry, DPTM), and a compliance culture that effectively balances strict enforcement with remedial flexibility. This model ensures robust customer privacy and corporate accountability, strengthening public trust in the digital economy.

Vietnam, while moving towards a centralized data regime (Decree 13/2023/ND-CP and the 2025 PDP Law), must learn from Singapore's experience to address institutional and capacity gaps. We recommend three core policy actions: Firstly, for institutional structure, Vietnam could consider establishing an independent administrative appeal body (study from DPAP) to ensure objective review of enforcement decisions, thereby bolstering transparency and investor confidence. Secondly, regarding governance capacity: Consider establishing a Specialized Data Protection Authority separate from the security apparatus to focus on compliance guidance, public education, and efficient dispute resolution. Thirdly, fostering compliance to gain proactive accountability by combining incentives and practical technical support for businesses with a mechanism that encourages self-reporting of minor breaches, moving away from a punitive-only approach. Future studies could quantitatively assess compliance costs for SMEs and analyze cross-border data governance capacity to ensure Vietnam's regulatory framework supports both national security and global digital trade.

REFERENCES

- Agc (2021). *Personal Data Protection Act 2012 (2020 revised edition)*. Available at: <https://sso.agc.gov.sg/Act/PDPA2012>
- Báo cáo EBI 2025 Final - Vn.pdf. Available at: https://drive.google.com/file/d/18hUNrKSJXQmKOQl7mLhghV1bg2MiKcmN/view?usp=drive_link&usp=embed_facebook (Accessed: October 22, 2025)
- baohinhphu.vn (2025). *Luật Thương mại điện tử cần bảo vệ người tiêu dùng, thúc đẩy thị trường số bền vững*. Available at: <https://baohinhphu.vn/luat-thuong-mai-dien-tu-can-bao-ve-nguoi-tieu-dung-thuc-day-thi-truong-so-ben-vung-102250905204814503.htm>
- Cahyaningsih, D.T., Kharisma, D.B. and Agnjana, G.A. (2024). “Urgency of E-Commerce Consumer Protection (Comparative Study in Indonesia, Singapore, and China).” *Pena Justisia: Media Komunikasi dan Kajian Hukum*, 23(2), p.141.
- Canhsatquanlyhanhchinh (2025). *Một số quy định đáng chú ý trong Luật bảo vệ dữ liệu cá nhân 2025*. Available at: <https://canhsatquanlyhanhchinh.gov.vn/gioi-thieu/mot-so-quy-dinh-dang-chu-y-trong-luat-bao-ve-du-lieu-ca-nhan-2025-3694>
- Chesterman, S. (2014). *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World*. Academy Publishing
- Chik, W.B. (2013). “The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform.” *Computer Law & Security Review*, 29(5), pp. 554–575.
- Consumer Protection. Available at: <https://www.mti.gov.sg/Resources/Legislation/Consumer-Protection>
- Dang Ngoc Dinh (2017). *Một số tiếp cận trong nghiên cứu chính sách*. Trung tâm Nghiên cứu Phát triển hỗ trợ cộng đồng, pp. 96–107
- Dário Moura Vicente, Sofia de Vasconcelos Casimiro (2020). *Data Protection in the Internet*. Available at: https://sci-hub.se/https://link.springer.com/chapter/10.1007/978-3-030-28049-9_13
- Data Security (2025). *Hơn 43% tổ chức, doanh nghiệp chưa có nhân sự chuyên trách bảo vệ dữ liệu cá nhân*. Available at: <https://datasecurity.vn/vi/post/hon-43--to-chuc--doanh-nghiep-chua-co-nhan-su-chuyen-trach-bao-ve-du-lieu-ca-nhan-26.htm>
- Electronic Transactions Act 2010 (2020 Rev. Ed.). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/Act/ETA2010>
- Foreign Interference (Countermeasures) Act 2021 (No. 34 of 2021). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/Act/FICA2021>
- Foxman, E. R., & Kilcoyne, P. (1993). “Information technology, marketing practice, and consumer privacy: Ethical issues.” *Journal of Public Policy & Marketing*, 12(1), 106-119.
- Goodwin, C. (1991). “Privacy: Recognition of a consumer right.” *Journal of Public Policy & Marketing*, 10(1), 106-119.
- Han (2024). ‘Ra mắt nền tảng tuân thủ bảo vệ dữ liệu cá nhân đầu tiên tại Việt Nam’, *Tạp chí Công Thương*, 6 June. Available at: <https://tapchicongthuong.vn/ra-mat-nen-tang-tuan-thu-bao-ve-du-lieu-ca-nhan-dau-tien-tai-viet-nam-122128.htm>

Huynh, T.T. (2025). *Everyone Is Safe Now: Constructing the Meaning of Data Privacy Regulation in Vietnam*. Available at: <https://www.cambridge.org/core/journals/asian-journal-of-law-and-society/article/everyone-is-safe-now-constructing-the-meaning-of-data-privacy-regulation-in-vietnam/85B4BA2CEDF2D4046CE076C11674E44C>

Info-communications Media Development Authority. (2023). *Data protection trustmark certification*. Available at: <https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification>

Info-communications Media Development Authority Act 2016 (2020 Rev. Ed.). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/Act/IMDAA2016>

International Business Law Program, Universitas Prasetiya Mulya ... and Ang, M. (2021). "Consumer's Data Protection and Standard Clause in Privacy Policy In E-Commerce: A Comparative Analysis on Indonesian and Singaporean Law." *The Lawpreneurship Journal*, 1(1), pp.100–113.

Karlengter (2013). *Singapore's Personal Data Protection legislation: Business perspectives*

Lanier, C. D., & Saini, A. (2008). "Understanding consumer privacy: A review and future directions." *Academy of Marketing Science Review*, 2008(1), 1-35.

Lanier, CD. Jr. and Saini, A. (2008). *Understanding consumer privacy: A review and future directions*. *Academy of Marketing Science Review*, 12(2), pp. 1-2

Law on Personal Data Protection 2025 No 91/2025/QH15 in Vietnam. Available at: <https://thuvienphapluat.vn/van-ban/EN/Bo-may-hanh-chinh/Law-91-2025-QH15-Personal-Data-Protection/665440/tieng-anh.aspx>

Le Van Tuyen (2022). *Thương mại điện tử ở Việt Nam - Thực trạng và Kiến nghị*. Khoa học xã hội Việt Nam

Li, Yubing. (2024). "An Exploration of Collaborative Governance of E-Commerce from the Perspective of Public Values." *E-Commerce Letters*, 13(02), 857–862.

Li, Z. (2023) "E-commerce Platform Data Governance Environment: Concepts, Elements and Implications," *Frontiers in Business, Economics and Management*, 7(2), pp. 99–104. Available at:

Milne, G. R., & Gordon, M. E. (1993). "Direct mail privacy-efficiency trade-offs within an implied social contract framework." *Journal of Public Policy & Marketing*, 12(2), 206-215

Minh Khoi (2021). "Singapore trao quyền kiểm soát Internet hơn cho các nhà chức trách." *Tuoitreonline*. Available at: <https://tuoitre.vn/singapore-trao-nhieu-quyen-kiem-soat-internet-hon-cho-cac-nha-chuc-trach-20211005112523885.htm>

Nguyen, H. and Vu, Y. (2025). *Vietnam's New Personal Data Protection Law: What Businesses Need to Know*. Available at: <https://rouse.com/insights/news/2025/vietnam-s-new-personal-data-protection-law-what-businesses-need-to-know/>

Nowak, G. J., & Phelps, J. (1995). "Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters." *Journal of Direct Marketing*, 9(3), 46-60.

OECD. (2021). *Going Digital to Advance Data Governance for Growth and well-being*.

OECD Publishing. https://www.oecd.org/en/publications/going-digital-to-advance-data-governance-for-growth-and-well-being_e3d783b0-en.html

Personal Data Protection Act 2012 (2020 Rev. Ed.). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/Act/PDPA2012>

Personal Data Protection (Appeal) Regulations 2021 (S 65/2021). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/SL/PDPA2012-S65-2021>

Personal Data Protection (Composition of Offences) Regulations 2021 (S 70/2021). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/SL/PDPA2012-S70-2021>

Personal Data Protection (Enforcement) Regulations 2021 (S 62/2021). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/SL/PDPA2012-S62-2021>

Personal Data Protection (Notification of Data Breaches) Regulations 2021 (S 64/2021). Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/SL/PDPA2012-S64-2021>

Protection from Online Falsehoods and Manipulation Act 2019 (2020 Rev. Ed.) Singapore Statutes Online. Available at: <https://sso.agc.gov.sg/Act/POFMA2019>

PDPC (2021). *PDPA Overview*. Available at: <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act>

PDPC | Accountability. Available at: <https://www.pdpc.gov.sg/help-and-resources/2021/09/accountability>

PDPC | PDPA Overview. Available at: <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act>

Quan điểm của Thương mại điện tử ở Việt Nam: thực trạng và kiến nghị. Available at: <https://vjol.info.vn/index.php/khxbvn/article/view/76038/64757>

Singapore Academy of Law (2014). *Data Protection Law in Singapore*. Available at: https://books.google.com.vn/books?hl=en&lr=&id=JSQUBAAQBAJ&oi=fnd&pg=PP1&dq=singapore+data+protection+law&ots=LKTzHTmXie&sig=z9UvmAiaWYbEchLv3oNRSOJoH0I&redir_esc=y#v=onepage&q=singapore%20data%20protection%20law&f=false

(PDF) “Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles” (2025) *ResearchGate* [Preprint].

Trang (2023). ‘Bảo vệ dữ liệu cá nhân-Nỗ lực bảo vệ quyền con người trong chuyển đổi số ở Việt Nam’. Available at: <https://ttdn.vn/nguyen-cuu-trao-doi/quyen-con-nguoi/bao-ve-du-lieu-ca-nhan-no-luc-bao-ve-quyen-con-nguoi-trong-chuyen-doi-so-o-viet-nam-79490>

Thu Phuong (2022). “*Thương mại điện tử xuyên biên giới trong khuôn khổ WTO, CPTPP và EVFTA*”. Available at:

https://scholar.dlu.edu.vn/thuvienso/bitstream/DLU123456789/175028/1/CVv225S92022055.pdf?fbclid=IwY2xjawOiIsRleHRuA2FlbQIxMABicmlkETFJMEclVzlodnB1Slg2d0pjc3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHqw4ovAHBPgQSTSLokqtA3MlstBZPwt7tN-bMBLCSOba2JX6VyH_Tl_00IZR_aem_U3q4AD6oPic-5MJKwhgVxA

UNCTAD. (2016). *Data protection regulations and international data flows: Implications for trade and development*. United Nations. <https://unctad.org/system/files/official->

[document/dtlstict2016d1_en.pdf](#)

Wang, H., Lee, M. K., & Wang, C. (1998). "Consumer privacy concerns about Internet marketing." *Communications of the ACM*, 41(3), 63-70.

World Bank. (2021). *World development report 2021: Data for better lives*. World Bank. <https://www.worldbank.org/en/publication/wdr2021>