기타보고서
2025-05

Designing Sustainable MyData Frameworks for Vietnam: A Comparative Study of Korea's Experience and Policy Adaptation for Local Innovation

2025.12

Nguyen Thi Minh Ngoc · Kwang Seok Choi

한국금융연구원

기타보고서
2025-05

Designing Sustainable MyData Frameworks for Vietnam:

A Comparative Study of Korea's Experience and Policy Adaptation for Local Innovation

Nguyen Thi Minh Ngoc* · Kwang Seok Choi**

* *National Credit Information Center of Vietnam, Research and Development Division, Principal Official*
** *Korea Credit Information Services, MyData Support Center, Credit Data Department, Manager*

CONTENTS

Designing Sustainable MyData Frameworks for Vietnam: A Comparative Study of Korea's Experience and Policy Adaptation for Local Innovation

Figure Contents

한국금융연구원 홈페이지(www.kif.re.kr 〉 보고서 〉 연구보고서)를 이용하시면, 본 발간물의 그림, 표를 컬러로 보다 상세하게 확인하실 수 있습니다.

I Introduction

1.1 Background of the Research

Along with the development of science and technology, especially in the era of technology evolution 4.0, humans' social and economic life experiences massive changes, more conveniently. Technology solutions weave through almost all aspects of daily life, such as in payment, communication, e-commerce, e-government, etc. The more people use technology daily, the more data is generated. According to Exploding Topics[1], an analytics company specializing in emerging trend identification, approximately 402.74 million terabytes of global data are generated daily, amounting to around 147 zettabytes annually. Since 2010, the volume of data produced has shown a consistent upward trend, with 90% of the world's data generated in just the last two years alone. Personal data is increasingly recognized as more valuable in the digital era, reflecting its rising significance and economic potential. As the digital economy advances, personal data increasingly signifies a valuable asset for individuals and a vital resource for organizations. This data facilitates greater access to a diverse customer base, enhancing and optimizing business strategies. However, the rapid expansion of cyber infrastructure presents numerous legal challenges, particularly concerning privacy rights, information security, and the obligations related to data protection. Thus, how to utilize data

1) Fabio Duarte (2025), "Amount of Data Created Daily (2024)". Exploding Topics, 8 March 2025, https://explodingtopics.com/blog/data-generated-per-day.

sufficiently and enhance data privacy creates double-sided issues.

In the context of technology development, digital transformation becomes an essential requirement for social and economic development, rather than an optional choice. Vietnam cannot step outside of this tendency since the country aims to convert innovation, digital transformation, and national science and technology development into the motivation and decisive factor for economic development[2]. As a key player in the global tech landscape[3], Vietnam has drawn an image of an active digital economy, especially in the finance and banking sector, with over 87% of adults having bank accounts, over 95% of transactions processed through digital channels in many financial institutions, and over 100% of annual average growth rate in mobile payment transactions and QR code payments in the phase of 2017–2023. In addition, banking technology infrastructure is regularly upgraded and developed. The interbank electronic payment system processes an average of VND 830 trillion per day (equivalent to US$40 billion), and the electronic clearing and settlement system processes an average of 20–25 million daily transactions.

However, due to the technology development associated with many potential risks, including misused and unauthorized identification utilization, and a lack of an efficient legal framework for personal data protection and sufficient financial education policies, financial consumers remain vulnerable in the digital finance and banking era, as evidenced by various factors.

Firstly, the increasing cases of misused and unauthorized identification

---

2) Resolution No.57-NQ/TW, signed by Party General Secretary To Lam on December 22, considers science and technology, innovation and digital transformation as the decisive factor for development.

3) Samaya Dharmaraj (2025), "Vietnam: A Major Player in the Global Tech Landscape". Opengovasia, https://opengovasia.com/2025/01/25/vietnam-a-major-player-in-the-global-tech-landscape, (accessed in June 29, 2025)

utilization in Vietnam, especially in financial transactions, have recently raised more concerns than before. The finance and banking industry remains the targeted sector for sales of personal information and corporate documents on various online platforms. According to the survey conducted in 2023 by the Global Anti-Scam Alliance (GASA) with the support of Chongluadao.vn, identity theft was among the top 3 most common scams in Vietnam and had the most impact compared to other types of scams. In 2024, 134 cases of data breaches potentially leading to misused and unauthorized identification utilization have been revealed in Viettel Threat Intelligence Report 2024, with approximately 294 million personal data records, equivalent to 184.3 gigabytes[4]. The case of data breaches in the sales service sector occupied the highest number, with 51 cases and 29 million personal data records. In addition, misused and unauthorized identification utilization has become a crucial link in the chain of financial scam processes. This deception created a barrier to hide the fraudsters' identities and trace the fraud-related transactions, such as making a fake account with a correct stolen ID card but a different ID image, utilizing proper banking accounts with unauthorized consent, etc.

Furthermore, the data subjects are still in a negative position to implement their data-related rights when dealing with misused and unauthorized identification utilization in Vietnam. There are no further options that support the data subjects in the case where their ID information has been misused or utilized without their proper consent, except for the advice of waiting for the investigation results from the Investigation Authority of the Ministry of Public Security if they report

4) According to Viettel Threat Intelligence Report 2024 published by Viettel Security. https://services.viettelcybersecurity.com/bao-cao-tinh-hinh-nguy-co-attt-vietnam-2024

their fraud cases. According to the GASA survey, reporting a minor loss is frequently challenging, time-consuming, and expensive.

Secondly, after the blooming of the internet in 2010, e-commerce and e-payment in the period 2020-2024, the Vietnamese government officially issued the first-ever regulation related to personal data protection, namely Decree No.13 dated 17 April 2023, followed by the Data Law issued in 2024 and Personal Data Protection Law approved by Vietnamese's Assembly in June 2025. However, during the implementation process, the current legal framework related to data privacy and protection has shown some obstacles and legal gaps regarding data control rights, responsibilities of all stakeholders, and detailed guidelines for implementation, which are regulated in the suitable sub-laws. Notably, the lack of the right to data portability leads to a competitive limitation in providing financial services and a less powerful condition of the data subject when controlling and managing their data.

Thirdly, the increase in identity theft cases has strong linkages with the lack of keen awareness of stakeholders involved in personal data protection issues, including data subjects and data processors. Specifically, Vietnam's population is ranked third in Southeast Asia and 16th globally, with 101 million in 2025[5], most of whom live in rural areas. A considerable number of citizens remain indifferent to the protection of their personal information, especially in cyberspace. Many still carelessly share their details on social media platforms, unconsciously click on harmful links, or even undoubtedly provide some essential information like OTP and account passwords, resulting in the leakage and exposure of sensitive data and indirectly exacerbating the pressing

5) https://www.worldometers.info/world-population/

issue of the illegal trading of personal information. In addition, the awareness of personal data protection among companies, enterprises, and financial institutions that collect, process, and utilize personal information remains limited. Moral hazard persists due to the absence of stringent internal regulations or appropriate training programs on personal data protection. In 2023, the Cybersecurity and High-Tech Crime Prevention Division (PA05) of the Da Nang Police Department dismantled a criminal network involved in the illegal collection and trading of bank account information, with the complicity of bank employees[6].

1.2 Purpose of Using Korea as a Reference Model and Research Questions

As aforementioned analysis, it is essential for Vietnam to establish an effective tool or platform that empowers data subjects to take control over their data protection, enhances awareness and insights regarding personal data protection, and strengthens legal rights and obligations, both in the technical and behavioral aspects, for all stakeholders involved. MyData industry in Vietnam remains the new concept, meanwhile it has been promoted and broadened in many countries around the world, proving its efficiency and benefits in creating a balance between data protection and data utilization, fostering a human-centric use of personal data, and strengthening the rights and obligations regarding personal data of all stakeholders, such as

6) Tuổi Trẻ. (2023). *Nhân viên ngân hàng bán thông tin tài khoản chỉ 200 000 đến 1,9 triệu/trường hợp*. Tuổi Trẻ Online. Retrieved June 29, 2025, from https://tuoitre.vn/nhan-vien-ngan-hang-ban-thong-tin-tai-khoan-chi-200-000-den-1-9-trieu-truong-hop-20230619222706361.htm

Kanta Services of Finland, MyData platform in Taiwan, MIDATA in Switzerland, and MyData platform in Korea. Outstandingly, the MyData platform in Korea, which was officially launched in 2022, can be considered a typical case study for countries like Vietnam, since Korea remains one of the few countries with a nationwide, cross-sector MyData platform, backed by legislative empowerment and an operational support platform. After three years of launching, starting with the financial MyData service, the MyData service in Korea has grown rapidly with cross-sectional approaches, including health, public, finance, telecom, and education sectors. The cumulative number of subscribers grew to about 165.3 million (as of May 2025), increased nearly 12 times from about 14 million users in January 2022. API (Application Programming Interface) daily transfers rose from 274 million in January 2022 to about 893 million in April 2025. MyData service providers also increased from 33 to 63 as of April 2025. In addition, the current financial infrastructure of Vietnam and Korea shows a number of similarities, such as centralized regulatory systems[7], financial ecosystemsdiverse mix of banks, fintech firms, insurers, and non-bank credit institutions[8], similar credit information systems, etc.

Thus, the research aims to examine the current data protection-related legal framework, conduct a comparative analysis of the potential

---

7) Both Korea and Vietnam operate under centralized regulatory systems, where the central bank plays a pivotal role in supervising the banking and financial services sector.
Korea: The Bank of Korea (BOK) oversees monetary policy, while the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS) handle regulatory oversight of banks and financial institutions.
Vietnam: The State Bank of Vietnam (SBV) functions both as the central bank and the key regulator for monetary policy, banking operations, and financial stability.

8) Financial ecosystems in both countries include a diverse mix of banks, fintech firms, insurers, and non-bank credit institutions. Both countries also show growing participation from non-bank players such as consumer finance companies, e-wallet operators, and peer-to-peer lenders, leading to the market diversification.

proposed MyData platform in Vietnam with the current one in Korea, to address two research questions, including:

(1) Why should the Financial MyData Platform be deployed in Vietnam with suggested operational structures from a similar platform in Korea?

(2) Which essential elements are needed to establish the MyData Platform initiative focusing on financial data in Vietnam?

1.3 Methodology and Scope

This study primarily adopts a qualitative legal research methodology, focusing on the analysis of Vietnam's current legal framework governing personal data protection and credit information activities, with particular attention to regulations relevant to the development of a Financial MyData platform. The research includes a comparative analysis of the international legal models, focusing on Korea's MyData legislation under PIPA and CIUPA, to identify best practices and potential adaptation pathways for Vietnam. Official legal documents, decrees, circulars, and publicly available guidance from regulatory bodies serve as the primary sources of analysis.

Due to the assigned functions and responsibilities of the State Bank of Vietnam (SBV), the study limits its scope to the financial sector, excluding broader cross-sectoral applications of MyData. The legal and institutional readiness of SBV and its affiliated entities, such as the National Credit Information Centre of Vietnam (CIC), is examined to assess feasibility within the current governance structure. The research also considers pilot program design elements and regulatory conditions necessary to support phased implementation.

Ⅱ Korea's MyData Platform – A Reference Model

As of the end of May 2025, there were approximately 165.31 million MyData service subscriptions. This indicates that, on average, individuals aged 14 and above who are eligible for MyData services are utilizing about 3.5 services each. The following section aims to provide an overview of Korea's MyData initiatives, covering its legal underpinnings, the diverse array of participants within its ecosystems, and the key services it provides.

2.1 Legal and Institutional Framework

Financial MyData services, often characterized as a "financial assistant in your hand," are seamlessly integrated into applications provided by banks, other financial institutions, FinTech firms, and even Big Tech companies. These services offer a unified view of financial information, allowing users to comprehensively manage their assets and liabilities, track expenditures, receive personalized financial product recommendations, and oversee their credit scores.

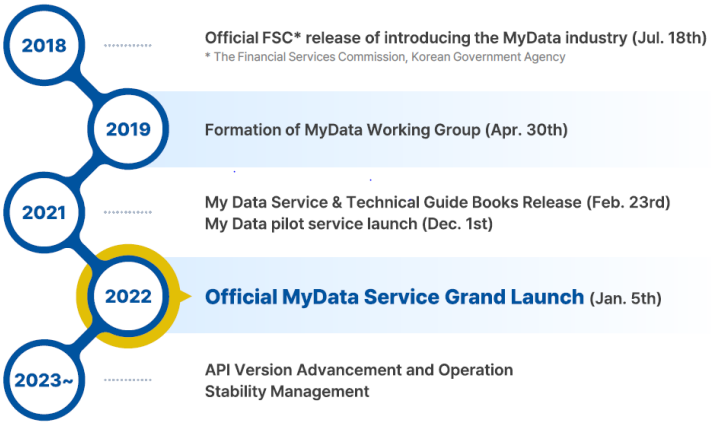
Korea has strategically embraced the MyData initiative as a cornerstone of its national agenda, aiming to propel the data economy and foster innovative digital governance. This commitment was formally articulated in June 2018, when the Presidential Committee on the Fourth Industrial Revolution unveiled its "Data Industry Revitalization Strategy." This seminal strategy laid the groundwork for establishing robust data portability and promoting the secure, judicious utilization of

personal information across diverse industries.

Beyond its foundational application in the financial sector, the MyData framework is being meticulously elaborated by various governmental ministries. The Ministry of Science and ICT is actively spearheading a MyData demonstration service project, showcasing practical applications. Concurrently, the Ministry of Interior and Safety commenced the development of a comprehensive public sector MyData distribution system, known as the MyData Portal, in 2020. Furthermore, the Ministry of Health and Welfare initiated the "My Healthway" system in 2021, a significant undertaking designed to facilitate the seamless integration and effective leverage of individual healthcare data.

In a pivotal move, financial regulators in July 2018 established the "Introduction Plan for the MyData Industry in the Financial Sector." This initiative was subsequently fortified by revisions to the Credit Information Act, which provides for the right of individuals to demand the transfer of their personal credit information and laid the groundwork for Personal Credit Information Management Businesses.

Figure 1. Timeline of Financial MyData Adoption in Korea



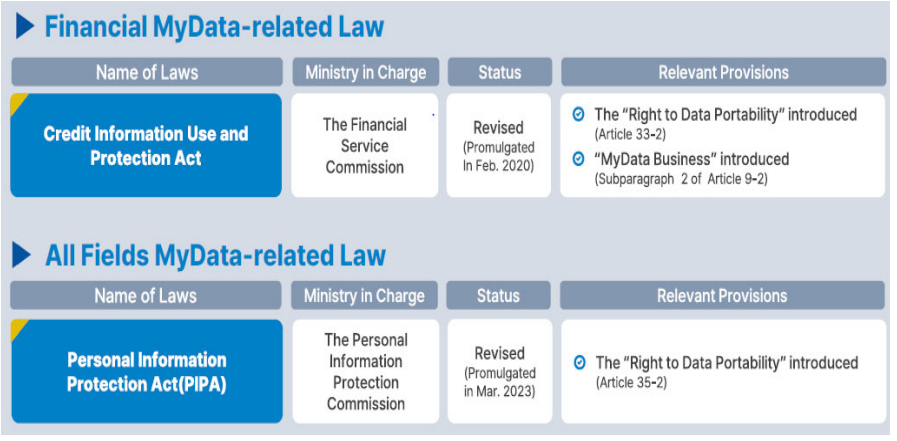
Source: Korea Credit Information Services

Financial MyData empowers consumers by facilitating credit information and asset management and enabling them to exercise their right to control their own information. It bears a strong resemblance to the Account Information Service Providers (AISPs) as defined within the EU's PSD2 framework.

MyData operators are uniquely positioned to serve as the primary interface. Their core function involves receiving fragmented personal credit information from financial institutions, via digital transfer, based on a customer's exercise of their data transfer rights. This data is then consolidated to provide the customer with integrated inquiry services. Beyond this core offering, MyData operators can also engage in ancillary and concurrent activities, including data analysis and consulting, third-party data provision, and asset management services such as investment advisory.

Given the substantial volume of personal credit information that MyData operators will aggregate and manage, financial authorities have opted for a licensing system. To qualify, MyData operators must satisfy

Figure 2. Regulatory Environments of MyData in Korea



Source: Korea Credit Information Services

stringent requirements, including the establishment of robust security frameworks for personal information management and breach prevention, rigorous conflict of interest prevention procedures, and the mandatory appointment of credit information management and protection personnel.

2.2 Governance and Ecosystem Actors

2.2.1 Korea's Financial MyData: Governance

Korea's financial MyData ecosystem is a sophisticated network designed to facilitate secure and consumer-centric data exchange. It's built upon a strong governance framework and involves various interacting actors.

These entities are responsible for establishing the legal and regulatory framework, setting policies, granting licenses, and ensuring compliance and stability within the MyData landscape.

1) **Financial Services Commission (FSC):** The primary policymaker and regulator for the entire financial sector. The FSC formulates MyData policies and leads the enactment/amendment of relevant laws like the Credit Information Act. It drives the strategic direction for financial innovation and consumer protection within MyData.
2) **Financial Supervisory Service (FSS):** The enforcement arm of the FSC. The FSS supervises and examines MyData operators to ensure their compliance with regulations, assesses their financial soundness, and plays a critical role in protecting financial consumers through inspections and regulatory actions.
3) **Personal Information Protection Commission (PIPC):** An independent

administrative agency governing personal information protection across all sectors in Korea. While the financial regulators focus on the financial domain, the PIPC ensures that MyData operations (including financial) adhere to the broader principles of the Personal Information Protection Act (PIPA). It's also instrumental in expanding the MyData concept beyond finance.

2.2.2 Korea's Financial MyData: Core Ecosystem Actors

These are the direct participants that drive the MyData service provision and consumption.

1) **Consumers (Data Subjects):** Consumers are at the very heart of the MyData ecosystem. They are empowered with the right to data portability, enabling them to control and demand the transfer of their own financial (and other) information from data providers to MyData service operators. They are the ultimate beneficiaries, using MyData services for integrated financial management, personalized product recommendations, and enhanced financial well-being. One of their key actions is granting consent for data transfer and utilizing MyData applications.
2) **Data Providers:** Data providers are the institutions that hold and generate consumer data. In the financial MyData context, this primarily includes banks, insurance companies, credit card firms, securities brokerages, and other financial entities. Importantly, in Korea, this also extends to relevant public sector institutions (e.g., for utility payment history, public pensions). They are legally mandated to provide requested data to MyData operators via standardized APIs upon consumer consent.
3) **MyData Service Operators:** These are the licensed entities (which

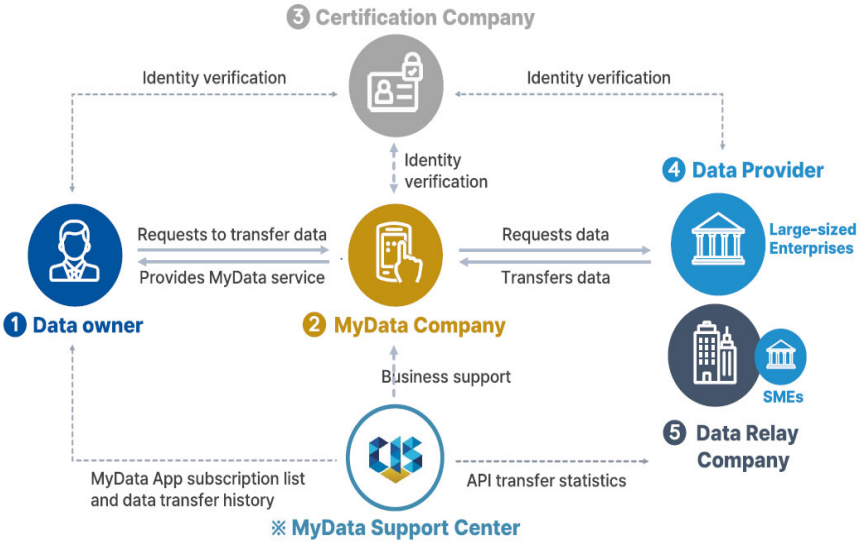
can include FinTech companies, Big Tech firms, or even traditional financial institutions that obtain a MyData license) that receive, aggregate, and manage individuals' financial and other personal data based on consumer consent. Their core businesses are providing integrated personal financial information inquiry services (e.g., consolidated asset/liability views).

4) **Certification Companies:** While not explicitly listed as a standalone MyData license category, "certification companies" often play a crucial support role within the ecosystem, particularly concerning authentication and digital identity verification. They provide the underlying infrastructure for consumers to securely consent to data transfers and authenticate themselves across various MyData services. This helps ensure that only the legitimate data subject is authorizing data access. Their key action is providing secure authentication solutions and digital certificates to verify user identity for data transfer requests.
5) **Key Data Intermediaries (Facilitating Secure Data Flow):** These entities perform vital functions to ensure the smooth, secure, and standardized flow of data within the ecosystem, often acting as bridges between data providers and MyData operators. Without them, MyData operators would face time-consuming and costly direct connections with each financial institution, leading to significant data interoperability challenges. Currently, there are 11 intermediaries in operation.
6) **Korea Credit Information Services (KCIS):** As the only Public Credit Registry(PCR) as well as the MyData Support Center, KCIS acts as an intermediary, facilitating the standardized API-based transfer of this comprehensive financial data to MyData operators, especially for smaller institutions in the insurance and installment sectors.

Furthermore, MyData Comprehensive Portal offers individuals convenient financial services, including integrated personal credit information inquiry and customized financial product recommendations.

7) **Financial Security Institute (FSI):** The FSI is responsible for the technical security framework of the financial MyData system. While not a direct data transfer intermediary in the same way as KCIS, FSI's role in developing security guidelines, conducting vulnerability assessments, and providing technical support is paramount to establishing and maintaining the secure environment in which all data exchange occurs.

Figure 3. Key Players in Financial MyData Ecosystem



Source: Korea Credit Information Services

2.3 Key Service Models and Business Cases

2.3.1 Legal / Regulatory Criteria

In Korea, MyData operates its function within a clear classification system defined by the Credit Information Act and its subsidiary regulations. This framework delineates their permissible activities into core, ancillary, and concurrent businesses, each with distinct regulatory requirements.

1) **The Core Business** is the fundamental activity for which a MyData license is required. It centers on receiving and processing an individual's personal credit information from various financial institutions, based on the "Right to Data Portability" exercised by the consumer. This involves providing an integrated view and management services for a consumer's entire financial portfolio (deposits, loans, investments, insurance, etc.) through a single platform. This is the primary service that necessitates stringent licensing and regulatory oversight due to its direct handling of highly sensitive personal financial data.
2) **Ancillary Businesses** are activities that are supplementary to the core business, often leveraging the data and capabilities acquired through it. These typically include data analysis and consulting for consumers, such as acting as proxies for data self-determination rights, providing advertising or consulting for financial products, and utilizing/providing pseudonymized or anonymized data to third parties. Historically, these required notification to the Financial Services Commission (FSC); however, recent regulatory discussions aim for more flexibility and a relaxation of explicit notification

requirements for certain ancillary services, recognizing their supportive role in the MyData ecosystem.

3) **Concurrent Businesses** encompass other types of operations, which can be financial or non-financial, conducted alongside the core MyData service. These are typically governed by specific financial laws (e.g., Investment Advisory, Electronic Financial Business, Loan Brokerage) or, if non-financial, are permitted as long as they are not explicitly prohibited by other laws and do not undermine financial soundness or consumer protection. Similar to ancillary businesses, the trend is towards a more permissive approach, where many concurrent activities may not require explicit prior approval, provided they adhere to general legal principles. The rigorous licensing process for the core MyData business implicitly covers the overall integrity and capability of the operator for these broader activities.

2.3.2 Service / Functional Criteria

MyData operators in Korea primarily offer the following core functionalities:

1) **Integrated Asset & Liability Management:** MyData platforms consolidate a user's entire financial portfolio from various institutions —including bank deposits, investments (funds, stocks), insurance policies, loans, etc. This provides a comprehensive, unified view of a user's total assets and liabilities.

   Examples: Seeing all bank balances, investment holdings, and outstanding loan amounts in one application. This is the most common model, with Big Tech leaders like Toss and Kakao Pay, as well as traditional financial institutions, evolving into holistic personal

financial management platforms.

Revenue Model: Commissions from promoting financial products, advertising, and premium subscription fees for advanced features.

2) **Expenditure Analysis & Management:** MyData operators integrate and analyze spending data from credit/debit cards and bank accounts to visualize and interpret consumption patterns. They provide insights into category-specific spending, trend analysis, and support budget setting and adherence, fostering more informed financial behavior.

   Examples: Detailed monthly breakdowns of spending on "dining" or "transportation," tracking expenditure changes from previous months, and monitoring budget achievement. These models extend beyond basic analysis to incorporate features like spending challenges, linking to micro-investment options, and incentivizing enrollment in financial products based on spending habits.

   Revenue Model: Targeted advertising derived from spending data, and commissions linked to financial product referrals.

3) **Personalized Financial Product Recommendations & Comparison:** By comprehensively analyzing a user's consolidated assets, liabilities, income, spending patterns, and financial activity (e.g., loan history, investment propensity), MyData operators deliver highly tailored recommendations for optimal financial products—be it deposits, loans, insurance, or investment instruments. They also facilitate direct comparison services, allowing users to easily evaluate features, rates, and terms across various products from different providers, moving beyond standard comparisons to offer "hyper-personalized" suggestions.

   Examples: Identifying the best debt consolidation loan, recommending higher-yield savings accounts, or suggesting insurance plans specific to an individual's age and health. This service is a core

revenue driver for comprehensive asset management apps and also underpins specialized advisory services.

Revenue Model: Affiliate commissions from financial product sales, and fees for premium financial/health consulting.

4) **Credit Score Management & Improvement:** Users can monitor their credit scores, understand the factors influencing them, and receive actionable advice on financial behaviors that can enhance their creditworthiness (e.g., timely debt repayment, prudent credit card use).

   Examples: Accessing credit score change history and receiving guides on how to improve one's credit standing. This service is often integrated into broader financial management apps or as a feature of loan/credit card services, aiming to foster financial health.

   Revenue Model: Drives user engagement and loyalty to the platform, potentially leading to cross-selling of other financial products or premium feature subscriptions.

5) **Notification & Assistant Services:** MyData platforms provide a range of customized alerts, including reminders for upcoming financial dates (e.g., payment due dates, interest receipts), notifications of asset fluctuations, warnings about potential overspending, and credit score updates.

   Examples: Alerts for credit card payment deadlines, stock account deposit notifications, or warnings about a credit score drop. These services enhance user experience and engagement, making the MyData platform indispensable for daily financial oversight.

   Revenue Model: Improves user retention and actively steers users toward other revenue-generating services on the platform.

2.4 Limitations & Challenges in Practice

While Korea's financial MyData industry holds a pioneering position globally, it nonetheless faces several limitations and challenges that must be addressed for its sustained development and the continued enhancement of consumer benefits.

2.4.1 Insufficient User Convenience and Activation

A significant barrier to entry for MyData services lies in the complex and extensive consent procedures. Users are often required to navigate numerous consent steps across various financial institutions and products, posing a particular challenge for digitally vulnerable groups, such as the elderly. Furthermore, as MyData services are primarily app-based, offline accessibility remains limited, hindering adoption by those less familiar with mobile environments. Some users also report a lack of substantial perceived utility beyond mere consolidated asset viewing, failing to derive genuinely impactful personalized services or meaningful financial insights. This contributes to the phenomenon of "dormant users" who cease engagement after initial sign-up. Technical issues, such as API call delays or communication inconsistencies, can also undermine service stability and user experience.

2.4.2 Difficulties in Securing Profitability and Issues with the Charging Structure

MyData operators currently grapple with a structural issue dubbed the 'cost paradox'. Since they incur API call fees for each data request, increasing user numbers lead to an exponential rise in API call volume, causing fixed costs to escalate disproportionately. This creates a scenario where expanding the user base could paradoxically exacerbate financial losses. Most MyData services are offered free of charge, with revenue predominantly relying on referral fees from financial product recommendations and brokerage. However, consumers often leverage MyData apps to check information and then independently seek more favorable products from other financial institutions, limiting direct in-app revenue generation.

2.4.3 Oversaturation of Operators

Despite its advanced state, Korea's financial MyData industry faces a significant structural limitation: an excessive number of operators relative to its market size. With around 65 Data operators currently competing for a limited domestic market and customer base, several issues are emerging. This intense competition severely exacerbates the challenge of achieving profitability. Given that most MyData services are offered free of charge, many operators, apart from a few large players or those targeting specific niches, struggle to secure a sufficient customer base or establish viable revenue models. They face increasing marketing costs for customer acquisition while finding it difficult to generate substantial revenue.

Consequently, this structural limitation is leading to business

withdrawals. The primary reasons behind companies like NHN Payco, KB FinTech, and FnGuide voluntarily relinquishing their MyData licenses in 2025 are precisely these mounting burdens of declining profitability and technology maintenance costs. Over-competition in the market can hinder long-term service innovation and investment, ultimately impeding the healthy development of the MyData industry. It's highly probable that more companies will exit the MyData business as the market undergoes further reorganization.

2.4.4 Constraints on Data Utilization and Scope Expansion

Currently, MyData predominantly focuses on financial information. However, integration with non-financial data intimately connected to daily life, such as retail, telecommunications, healthcare, and energy, remains limited. While integrating such information is crucial for MyData to evolve into a true "life-centric financial assistant," expansion is complicated by potential conflicts with the Personal Information Protection Act and sector-specific regulations. Concerns also persist regarding data sovereignty and potential misuse. There is apprehension that individuals, in consenting to provide vast amounts of data for service use, may not fully understand how their information is being utilized, or that excessive and unnecessary data could be collected. Consumer and civic groups consistently raise issues about data leakage, misuse, and commercial exploitation. Furthermore, information providers (financial institutions) face burdens related to the costs of building and maintaining systems for data provision, coupled with concerns about increased competition and potential customer attrition due to data being shared with rival apps.

2.4.5 Regulatory Environment Challenges

Initially, the regulations governing the scope of MyData operators' concurrent and ancillary businesses were relatively rigid, limiting the development of innovative business models, including those aimed at becoming "killer services". While recent efforts aim to relax these regulations, some argue they still do not fully reflect market demands. There is also a perceived lack of a fair compensation mechanism for data providers (individuals and institutions), which could diminish the incentive for data sharing if the value of the data is not appropriately recognized and compensated. Lastly, Korea's MyData framework is primarily rooted in the Credit Information Act, differentiating it from GDPR-based data portability frameworks in other countries. This distinction may necessitate further discussion regarding global data linkage and interoperability in the future.

2.5 Implications for Policy Adaptation

2.5.1 Proactive and Agile Regulatory Leadership

The Korean case powerfully demonstrates that a strong, proactive, and centrally coordinated government role is paramount. It involves establishing a clear, robust legal and regulatory foundation from the outset, actively driving cross-sector participation, and mandating technical standards (like API-based data transmission) to ensure uniformity, interoperability, and security across the ecosystem. A prime example of this proactive approach was the Korean government's early formation

of active operation of working groups composed of participating institutions to drive data standardization. However, this leadership must also be adaptive, capable of rapid iteration and modification in response to market feedback and unforeseen challenges, rather than maintaining rigid control.

2.5.2 Embrace Economies of Scope through a Comprehensive Inclusion of Available Data Sets

Unlike major economies such as the EU and the UK, where MyData initiatives primarily centered on sharing bank payment account information, Korea's financial MyData industry distinguishes itself through a significantly broader scope of shared data. This encompasses information from banks, insurance companies, credit card firms, securities brokerages, and even the public sector.

Maximizing the utility of MyData hinges on a comprehensive approach to data inclusion. Governments should consider the broadest feasible scope of data from the start, extending beyond basic financial transactions to encompass a wide array of financial products (investments, insurance, loans) and potentially even relevant non-financial or public sector data. This foresight fosters richer insights, enables more sophisticated integrated services for consumers, and creates a robust foundation for future innovations. A phased approach might be considered, but with a clear roadmap for expansion, ensuring the framework is scalable and adaptable to evolving data landscapes.

2.5.3 Strategically Balance Robust Data Protection with Innovation Catalysis

This is perhaps the most critical and delicate balancing act. While robust data protection mechanisms (like strong consent frameworks and security protocols) are non-negotiable for building trust and ensuring ethical data use, policymakers must also ensure that regulations do not inadvertently stifle innovation. Overly rigid or prescriptive regulations, particularly concerning the scope of ancillary and concurrent business activities, can constrain operators' ability to experiment, develop novel business models, and create truly differentiating "killer services." Future regulatory frameworks should strive for inherent flexibility, enabling experimentation and the organic evolution of services within clearly defined ethical boundaries and robust consumer protection safeguards, perhaps through sandboxes or iterative pilots.

2.5.4 Implement Prudent Market Sustainability Planning

The Korean experience with market oversaturation serves as a significant cautionary tale. Policymakers should meticulously consider the optimal number of licensed operators relative to the projected market size and demand. An overly permissive licensing approach, without corresponding market depth or clear pathways to profitability, can lead to debilitating over-competition, market fragmentation, and widespread business exits, ultimately undermining the stability and confidence in the ecosystem. Strategies for market evolution, including potential consolidation or diversification incentives, should be considered from the outset.

2.5.5 Actively Foster Diverse Monetization Strategies for Operators

To ensure the long-term viability of MyData ecosystems, governments and regulators must actively encourage and facilitate the development of a wide array of revenue streams for operators. Relying solely on free services and basic referral fees may prove unsustainable for many players. Policies should support models that enable value-added services, premium offerings, or innovative data-driven insights that consumers are willing to pay for, directly or indirectly. This diversification of revenue streams is crucial for attracting sustained investment, fostering continuous innovation, and building a resilient MyData industry.

2.5.6 Prioritize User Experience and Engagement

Beyond regulatory and technical aspects, the success of MyData hinges on widespread user adoption and continuous engagement. Policies should push for simplified consent processes, intuitive user interfaces, and demonstrable and tangible benefits for consumers that go beyond just data aggregation. Addressing issues like "dormant users" and ensuring accessibility for all demographics, including digitally vulnerable populations, is vital. Proactive government communication and education campaigns can also play a significant role in building public awareness and trust.

By meticulously learning from both the triumphs in ecosystem participation, data scope, and standardization, and the tribulations in market sustainability and profitability faced by Korea's MyData journey, other governments can strategically design policies that effectively

unleash the full potential of personal data. This approach can empower consumers by granting them greater control over their information, while simultaneously building a robust, innovative, and sustainable data-driven economy for the future.

Ⅲ Vietnam Country Report

3.1 Vietnam-Specific System and Readiness Analysis

3.1.1 Legal and Data Protection Framework

a. General data-related legal framework

Vietnam's legal system related to personal data protection is built on a multi-layered model, in which each regulation plays a vital role in creating a comprehensive legal framework. The 2013 Constitution, as the highest level basis for personal data protection, Article 21, affirms the right to inviolability of private life. This provision is particularly important when it sets out state agencies and organizations' obligations to protect citizens' data. The 2015 Civil Law specifies this right in Article 38, regulating the right to privacy and personal secrecy, and at the same time defines prohibited acts such as illegally collecting, storing, using, or disclosing personal information. In addition, the Civil Law also stipulates the responsibility to compensate for damages if this right is violated, creating a mechanism to protect individual rights.

Following the global trend of establishing a modern IT infrastructure and enhancing information technology development, for the first 20 years, Vietnam has focused on establishing the legal framework for IT infrastructure development and digital transformation rather than the digital data itself. The issues related to data privacy, data protection, and data subjects' rights have raised more concerns and have been

strictly regulated since 2023 by issuing Decree No.13 on personal data protection.

The initial phase of data-related regulation in Vietnam was marked by laws that were not solely focused on data protection, but laid the essential groundwork for subsequent, more targeted legislation to establish and develop the IT infrastructure in Vietnam. The Law on Information Technology[9] (IT Law), Law on Cyber Information Security[10] (LOCIS), and Law on Cybersecurity (LOCS)[11] remain notable regulations in this period.

- IT Law, effective January 1, 2027, was one of Vietnam's earliest legislative efforts to address the burgeoning digital environment. It established overarching principles for developing, managing, and utilizing information technology across various societal sectors, including government, business, and education. Crucially, the IT Law introduced foundational concepts related to data, including provisions for data protection, such as the requirement to obtain consent from individuals before collecting, using, or disclosing their personal information. It also touched upon intellectual property rights in the IT domain and measures to combat cybercrime. The law's stated aims were to foster a legal IT framework conducive to socio-economic development while ensuring communications and IT systems' security, safety, and confidentiality. While its data protection provisions were less comprehensive by contemporary standards, the IT Law was significant for introducing the principle of consent for personal data handling. However, it was limited to the basic concepts regarding collecting, processing, and utilizing other personal data and providing

9) No. 67/2006/QH11

10) No. 86/2015/QH13

11) No. 24/2018/QH14

it to third parties.

- LOCIS was issued in 2015, representing a more direct step towards modern data protection. This law focused on ensuring network information security, encompassing protecting personal information online. The LOCIS also enabled Data Subject Request (DSR) automation, allowing individuals to request access, update, alteration, or deletion of their personal information. Unlike the subsequent Cybersecurity Law, which strongly emphasizes state control over information flows, the LOCIS was geared more towards enforcing data privacy rights for individual data subjects. It mandated that organizations handling personal data implement security measures and reiterated the necessity of obtaining consent before processing personal data, including its collection, modification, use, storage, provision, sharing, or transmission.
- LOCS, effective January 2019, was enacted to safeguard national security and social order within cyberspace while protecting stakeholders' legitimate rights and interests, including those of organizations and individuals. Key provisions of the LOCS include stringent data localization requirements, mandating that certain types of data, such as personal information, data on user relationships, and data generated by users in Vietnam, be stored within Vietnam. These requirements apply to both domestic and foreign enterprises operating in specified sectors. In addition, the government issued several relevant sub-law documents, such as Decree No.85 on the security of information systems by classification with five tiers. Based on each tier, the different requirements for information security are applied, from basic to complex.

Following the established foundation regarding data-related legal framework, recognizing these challenges, and aligning with evolving

international and regional standards[12], Vietnam began to focus on data governance with a multi-layer legal framework. The initial and remarkable effort of the Vietnamese government regarding the legal framework strengthening towards data protection is the birth of Decree No. 13/2023/ND-CP on Personal Data Protection (DPDP).

Indeed, DPDP is considered the first comprehensive regulatory framework dedicated solely to personal data protection, which firstly introduces key definitions including personal data, sensitive data, data controller, and data processor, indicates the rights of data subjects, establishes stringent requirements for obtaining consent, mandates data processing impact assessments, and regulates cross-border data transfers. Notably, DPDP also prohibits the buying and selling of personal data, except where permitted by law. DPDP, effective July 1, 2023, brings Vietnam's data legal framework closer to international standards (e.g., EU's General Data Protection Regulation – GDPR). Some critical terms, such as "personal data" including "basic personal data" and sensitive data", "data controller", "data processor", and personal data processing" have been clearly defined. Furthermore, the PDPD mandates the completion of Data Protection Impact Assessments (DPIAs) for high-risk processing activities and Data Transfer Impact Assessments (DTIAs) for the cross-border transfer of personal data. The decree possesses an extraterritorial scope, applying to foreign agencies, organizations, and individuals directly participating in or related to personal data processing activities in Vietnam, irrespective of their physical presence there.

After nearly two years of implementing the DPDP and incorporating

12) Including later ASEAN initiatives that placed greater emphasis on data protection, such as the ASEAN Framework on Digital Data Governance (2018) and the ASEAN Agreement on Electronic Commerce (2019) which explicitly mentions the protection of personal information of e-commerce users.

feedback on the requirement for a higher-level legal framework, the National Assembly of Vietnam officially passed the Personal Data Protection Law (PDPL) on June 26, 2025, following four rounds of draft submissions. In the comparison with DPDP, PDPL brings more significant changes, including the extension of the regulated scopes[13], the clarity improvement and supplementation of some definitions (e.g., personal data pseudonymization), higher penalties to enhance deterrence[14], and detailed regulation regarding data processing in high-tech required sectors. PDPL maintains the obligations for DPIAs and DTIAs when processing and transferring cross-border data. Notably, PDPL has adjusted and added 9 new provisions regulated data protection issues regarding some specific data subjects (e.g., children, people with lost or limited civil capacity, and people with difficulty in cognition and behavior control), and in some specific activities (e.g., recruitment, management and use of employees; health information and in insurance business; financial, banking and credit information activities; advertising service business; social networking platforms and online media services; big data processing, artificial intelligence, blockchain, virtual universe and cloud computing; location data and biometric data; and recording and filming in public places and public activities). PDPL has restructured the regulation related to the rights of data subjects, from 11 rights in PDPD to 6 rights in PDPL, including (i) the right to be aware of personal data processing activities, (ii) the right to consent or reject the personal

13) PDPL expands the scope of application, especially targeting foreign organizations and individuals without a presence in Vietnam but processing data of Vietnamese citizens or people of Vietnamese origin whose nationality has not been determined. Thus, international social media platform like Google, Facebook, Tiktok will operated under this regulation if proccessing Vietnamese citizens' data.

14) Maximum fines are up to VND 3 billion for common violations; 5% of previous year's revenue for cross-border data transfer violations; and 10 times the revenue from illegal data trading.

data processing activities, and to withdraw the consent at any time; (iii) the right to view, edit and request the correction of personal data; (iv) the right to request the provision, deletion, or restriction of personal data processing activities and to object to such processing; (v) the right to file complaints, make denunciations, initiate legal processing, and seek compensation for any damage as provided by law; (vi) the right to request competent authorities, organizations, or individuals, who involved in data processing, take appropriate measures to protect their data under the law. Especially, "the right of data deletion" which similar to "the right to be forgotten" regulating in Article 17, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679[15], is controlled more detailed in Article 14 of PDPL about "Personal data deletion, destruction, and pseudonymization".

In addition, before issuing the PDPL, Vietnam has also moved towards enacting an even more comprehensive Data Law, which comes into effect on July 1, 2025. This law aims to govern digital data more broadly, encompassing aspects of data ownership, establishing a national data center, and further clarifying personal and non-personal data regulations. This is a landmark legislation as it is Vietnam's first comprehensive law governing data in general, extending beyond the scope of personal data to encompass all forms of digital information. Key provisions of the Data Law include the groundbreaking recognition of "data ownership" as a property right under civil law, granting data owners full authority to manage, protect, use, and

15) Article 17, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 indicates that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" in some specific circumstances. The right to be forgotten is also applicable in some countries' legal framework, such as Brazil, although it is not explicitly named, or in other countries like Colombia and Argentina, based on specific judicial precedents.

exchange their data. The law introduces definitions for "digital data." It establishes critical classifications such as "important data" and "core data". These classifications are pivotal as they trigger specific, often stricter, cross-border data transfer and processing requirements. The Data Law also mandates periodic risk assessments for entities handling important or core data. It defines various data products and services, such as data intermediary services, data analysis and aggregation, data trading platforms, and electronic authentication services, with specific restrictions on which entities (primarily state-owned enterprises and public sector entities) can offer data trading platforms and authentication services.

Furthermore, the law lays the legal foundation for establishing a National Data Centre and a National General Database to improve state management and facilitate data integration. The Ministry of Public Security (MPS) is designated the primary state agency responsible for data management under this law, consistent with the regulation of PDPL as the primary state agency for data protection. This legislation signifies a significant expansion of data regulation, aiming to govern the entire data lifecycle and strategically harness data as a national asset, while concurrently imposing new and considerable compliance obligations related to data classification, ownership, and cross-border data flows.

b. Data-related regulations in the finance and banking sector

In the finance and banking sector, personal data protection is also regulated under the Personal Data Protection Law, Data Law, and Law on Credit Institutions (LoCI), and Decree No. 117/2018/ND-CP[16], which

16) Decree No. 117 /2018/ND-CP issued in 2018 by the Prime Minister on the protection of confidentiality and provision of borrowers' information of credit institutions and foreign banks' branches.

have the highest legal validity in the current data-related legal system. The LoCI indicates the standard rules on information confidentiality, data safety, and assurance of continuous operation by following financial data regulations. As mentioned above, PDPL has a specific provision regulating personal data protection in the finance, banking, and credit information sectors. According to that, organizations and individuals operating in the financial, banking and credit information sectors shall have the following responsibilities, as follows: (i) fully comply with regulations on protection of sensitive personal data, safety, and security standards in financial and banking activities as prescribed by law; (ii) do not use credit information regarding the data subjects to conduct credit rating, credit scoring and credit information and creditworthiness assessment without their consents, (iii) only collect personal data necessary for credit information activities from sources under the provisions of this Law and other relevant legal provisions; (iv) notify the personal data subject in case of disclosure or loss of information on bank accounts, finance, credit, and credit information. In addition, credit institutions and foreign banks' branches shall promulgate internal regulations on the protection of confidentiality, storage, and provision of client information and uniformly organize the implementation (regulated in Decree No. 117/2018/ND-CP).

At the sub-law level, due to the specific nature of the banking sector, the State Bank of Vietnam has issued several particular regulations to govern data handling, cybersecurity, and operational risk within the payment services sector inside the banking system, such as Circular No.17 dated June 28, 2024 on opening and using payment accounts and Circular No. 50 dated October 31, 2024 on providing for security and confidentiality during provision of online banking services.

According to Circular No.17, "Cash withdrawal and e-transactions

made via checking accounts are only allowed when personal information documents and biometric information of account holders or representatives (for individual customers) or legal representatives (for organization customers) are cross-checked"[17] and "Banks and Foreign Banks' branches must monitor effective period of personal documents of account holders and relevant persons in the use of checking accounts; notify customers at least 30 days before expiry of personal documents for update and revision; suspend all payment and cash withdrawal transactions via checking accounts if personal documents of customers expire[18]". As a result, 37.4 million customers have successfully registered their biometric information, which will be cross-checked and integrated with their bank accounts after 2 months of implementation. The account holders must verify identification information if making a transaction of over VND10 million or over 20 million VND daily. They cannot withdraw or make any transaction if they fail to provide biometric information associated with their accounts.

Circular No. 50, effective January 2025, issued by the Governor of the State Bank of Vietnam, regulates security and confidentiality while providing online banking services. This circular significantly modernizes and expands the security requirements for online financial services, with the scope extending beyond traditional banking and payment services to include credit information services, foreign exchange services, securities depository services, and services related to factoring and letters of credit. A key regulated feature is the mandate for a risk-based approach to transaction authentication: simpler methods like passwords or PINs are permissible only for small-value online

17) Point c, Clause 5, Article 17

18) Clause 3, Article 19

transactions, while larger-value or higher-risk transactions require more robust forms of authentication, such as One-Time Passwords (OTPs) delivered via SMS, voice, or email, biometric matching, or e-signatures. The circular also requires adherence to technical standards, such as implementing firewalls and DMZ (demilitarized zone) network barriers[19].

3.1.2 The Maturity and Readiness of the Current Legal Framework

With the regulated scopes of PDPL and Data Law, Vietnam has created a strong foundation for the personal data-related legal framework. Thanks to this foundation, the legal framework regarding data protection could be expanded further with the contribution of upcoming sub-laws issued by the Vietnamese Government and other ministries. For example, according to some articles of the PDPL, the Vietnamese Government is assigned to issue the necessary sub-laws which will regulate some specific aspects, such as the form of data subjects' consents, the activities regarding personal data transfer and cross-border data transfer, guidelines on documentation, conditions, procedures, processes for conducting DTIAs and DPIAs, and the activities of data protection in the finance, banking and credit information sector.

The availability of some factors (e.g., the regulation of data protection during the personal data processing procedures, and the regulation related to data-related products and services, including electronic authentication, data intermediation, and data analysis and aggregation services) contributes to facilitating the establishment of the Financial MyData platform in Vietnam. However, in comparison with other

19) Clients' information including identification information, transaction data is not allowed to store in the Internet connection zone and demilitarized zone (DMZ).

countries or regions' legal framework regarding personal data protection, such as Korea, Finland, Singapore, Europe, etc., there is a need for improvement of Vietnam's current legal framework, especially targeting the established direction of the Financial MyData platform here. Thus, the evaluation of the maturity and readiness of the current legal framework related to data protection in Vietnam can be considered as follows:

Firstly, thanks to the issuance of the Data Law and Personal Data Protection Law as the strong foundation for the data protection-related legal framework, Vietnam has accumulated some other essential conditions for establishing a Financial MyData platform. Specifically, Articles 39 to 42 of the Data Law have detailed regulations regarding data-related products and services, including electronic authentication services, data intermediation services, data analytics and aggregation services, and data trading platforms. The rights of data subjects and the obligations of all stakeholders involved in the data protection activities have been well-regulated.

In the finance and banking sector, Decree No. 94/2025/ND-CP ("Decree 94") was issued to establish a controlled testing environment, so-called "Regulatory Sandbox" for Fintech solutions in the banking sector. It will enable a regulatory framework and an implemented environment for data sharing via Open Application Programming Interface (Open API)[20], an essential factor in establishing the Financial MyData platform. Accordingly, financial institutions, customers, and related third parties shall "comply with the law on protecting and providing customer data and personal data protection. The processing of a customer's data serves only the respective customer, unless

20) Data Sharing via Open Application Programming Interfaces (Open APIs): Solutions enabling secure data exchange between banks and third-party providers, based on customer consent.

otherwise prescribed by law". Before that, the State Bank of Vietnam had issued Circular No. 64/2024/TT-NHNN dated December 31, 2024, on implementing Open APIs in the banking sector. Principles of the implementation of Open APIs, the list of basic Open APIs (e.g., API for authorization and consent, Open APIs for payment initiation, etc.), and technical standards regarding Open APIs in the banking system have been specified in this regulation.

Secondly, a lack of some essential regulations regarding the data subjects' rights in Vietnam could diminish the power of data subjects in data management, control, and protection in a flexible way. The current regulations regulating data subjects' rights do not include the "right of data portability," which is considered a powerful right to support the data subjects in effective data management, control, and protection. The right of data portability, which is first regulated in Article 20, GDPR (EU), is also the essential right of data subjects in the global scope. This right ensures that individuals can receive their data in machine-readable formats and easily and interoperably transfer data among data providers without interruption or loss. In addition, in the right circumstances, data portability has the potential to boost competition, foster data-driven innovations, and broaden consumer choice (Reimsbach-Kounatze, C., A. Molnar, 2024)[21]. Although enabling the right of data portability does not guarantee the success of human-centric data protection, this critical right is an essential condition to establish and foster MyData services. The success depends on the effective and secure implementation of the data request and transfer processes in line with privacy and data protection

21) Reimsbach-Kounatze, C. and A. Molnar (2024), "The impact of data portability on user empowerment, innovation, and competition", OECD Going Digital Toolkit Notes, No. 25, OECD Publishing, Paris, https://doi.org/10.1787/319f420f-en.

obligations and best practices (Reimsbach-Kounatze et al., 2024).

Thirdly, the role of specific supervisory and implementation authorities is not indicated clearly in the scope of the data-related legal framework. Despite PDPL having been issued targeting to be the higher-level personal data protection legal framework, inheriting the majority of related regulations from Decree No.13 on personal data protection, PDPL remains complex in supervision and implementation of data protection activities. Specifically, Article 36 of PDPL indicates that the Ministry of Public Security is the focal agency that takes charge of data protection, except for the data in the protected scope of the Ministry of Defense. Meanwhile, other ministries, ministerial-level agencies, and government bodies are responsible for overseeing personal data protection within their assigned sectors and areas of regulation. Provincial People's Committees also carry out state personal data protection management following their delegated responsibilities.

Thus, this situation may lead to a fragmentation of authority, overlapping functions in state management, and a lack of uniformity in supervision, creating more difficulties for individuals and businesses in identifying the competent authority to handle complaints or provide legal guidance on personal data protection. For example, in the telecommunications sector, Vietnam has three major telecommunication companies named Viettel, Vinaphone, and Mobifone, which are operated under the management and supervision of the Ministry of Defense, the Ministry of Finance, and the Ministry of Public Security, respectively. If subscriber information is leaked due to the fault of a telecom provider, each ministry takes charge of management and supervision, and can be responsible for handling the issue. However, if the leaked data is exploited for fraudulent purposes, the investigative authority under the Ministry of Public Security holds jurisdiction.

Similarly, the State Bank of Vietnam may play a supervisory role if customer data is compromised due to a cyberattack in the finance and banking sector. Still, if the violation involves financial fraud, the responsibility lies with the Ministry of Public Security (Tran Thi Thanh Bich, Dao Thi Anh Thu, 2025)[22].

Fourthly, on the scale of global data protection-related legal frameworks, many countries (especially those with strict regulations on data protection) have designated independent authorities or state agencies tasked with overseeing data protection laws, regulating personal data handling, and resolving consumer complaints or disputes related to data protection. However, Vietnam's current legal framework regarding personal data protection does not provide more detailed regulations. The European Union (EU) requires each member state to have a national Data Protection Authority (DPA) responsible for supervising the implementation of the GDPR (EU)[23], handling complaints related to personal data breaches, issuing compliance guidance to businesses, and coordinating with other DPAs across the region to ensure legal consistency throughout the EU. Regionally, each country, like Korea, Japan, Singapore, the Philippines, and Thailand, has its independent agency that typically implements the following functions: handling complaints from individuals (data subjects), investigating breaches of data protection laws (if any), issuing fines or sanctions, auditing organizations that perform data-related activities, provide supports in increasing finance literacy and leverage the awareness and

22) Tran Thi Thanh Bich, Dao Thi Anh Thu (2025), "Pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam, Những khoảng trống và hướng hoàn thiện". Luật sư Việt Nam. https://lsvn.vn/phap-luat-ve-bao-ve-du-lieu-ca-nhan-o-viet-nam-nhung-khoang-trong-va-huong-hoan-thien-a156811.html (Accessed on July 5, 2025).

23) List of national Data Protection Authority in each European countries: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

responsibility of all stakeholders involved, and ensuring international compliance with the best practices or standards (e.g., GDPR). In Korea, the Personal Information Protection Commission (PIPC) is a notable example of a strong, independent authority established to consolidate data protection enforcement, especially after amendments to PIPA in 2020.

Additionally, Article 34 of the Personal Data Protection Law (PDPL) of Vietnam only regulates standards and technologies related to data protection. It does not specify which state agencies or specialized organizations will be responsible for developing these standards. Meanwhile, Korea Financial Security Institute (FSI), which is a specialized organization under the Financial Services Commission (FSC), serves as the financial sector's dedicated cybersecurity and information protection institution. FSI plays a critical supporting and supervisory role in ensuring the security, integrity, and reliability of personal financial data services in Korea, and it acts as the backbone of cybersecurity, compliance, and operational resilience within the MyData infrastructure.

3.1.3 Identifying Integration Challenges within the Banking Ecosystem

With the legal framework on personal data protection in Vietnam approaching its maturity, establishing and developing the Financial MyData platform presents a promising and worthwhile opportunity for advancement. However, this promising initiative shows some challenges as foreseen based on the implemented experiences from prominent countries in this area.

First, the legal framework regarding personal data protection needs to be revised and adjusted to facilitate the Financial MyData platform.

However, the revision process usually takes longer than expected due to the many layers of approval in Vietnam's legal system, with several rounds of feedback from all stakeholders involved. Without the support from the regulators at the state level, the perfection of the data-related legal framework is a big challenge to establishing the initiative of the Financial MyData platform. Moreover, harmonizing sectoral regulations, such as banking, cybersecurity, and digital identity, is essential to avoid legal fragmentation and ensure coherent implementation. The lack of clearly defined responsibilities among state agencies may also lead to overlaps or regulatory gaps, confusing service providers and users. Compared to other countries like Korea, where legal adjustments were prioritized early in the MyData rollout, Vietnam still faces significant delays in aligning its regulatory structure. These legal uncertainties may discourage potential investors and stakeholders from engaging in pilot projects or system development. Therefore, proactive leadership from state authorities and a roadmap for legal harmonization are crucial to accelerate the transition toward a functioning Financial MyData platform.

Second, regarding some common challenges that most countries need to face, data standardization is the primary concern for most countries trying to establish the initiative of the Financial MyData platform. Currently, each bank or financial institution operating in Vietnam has its own systems or protocols, leading to several constraints when conducting periodic reports to the State Bank of Vietnam. Each report requires a specific list of indicators, which may change depending on the SBV's requirements. In this case, financial institutions typically extract needed information via intermediation applications built internally or provided by third parties. Data standardi-zation and integration are also costly and fragmented, especially

becoming a financial and technical burden to small financial institutions. The lack of data standardization also deteriorated the capacity to update information supporting the SBV's state management function and provide products and services to the customers based on real-time data. Currently, the SBV is now on the way to promoting data standardization in the banking sector, which is marked with the project funded by the World Bank named "Assessment of the Current State of the Shared Specialized Banking Database", financed by the World Bank and consulted by KPMG Vietnam. However, data standardization and integration continue to pose significant challenges for the banking sector, particularly as an increasing number of participants, such as fintech companies, join the ecosystem to build a comprehensive financial and banking information system.

Third, according to the Going Digital Toolkit note named "The impact of data portability on user empowerment, innovation, and competition", established in 2024 by the OECD, data portability can be improved by a step-by-step method, including ad hoc data downloads (version 1.0), ad hoc direct transfers of data to another data holder for (version 2.0), and real-time continuous data transfer enabling interoperability for (version 3.0). If the right of data portability is considered to be added to the current legal framework regarding personal data protection, the requirement of data erasure and transfer without undue delay, following the international practices (e.g., GDPR – EU; PIPA – Korea, etc.), poses more challenges related to the need of thorough preparation for the development of Financial MyData platform in the long-term. These preparations are strongly linked with the vision of the high-level regulators, the strategy of establishing the MyData platform on a cross-sector scale, and insights learnt from experiences of other countries with successful MyData industries.

Fourth, the benefit and profitability guarantee mechanism for all stakeholders involved is a direct challenge to implementing the initial step of establishing the Financial MyData platform. As discussed above, robust data protection mechanisms (like strong consent frameworks and security protocols) are non-negotiable for building trust and ensuring ethical data utilization. Policymakers must also ensure that regulations do not inadvertently stifle innovation. Thus, how to research and introduce the benefit and profitability guarantee mechanism to ensure the benefits to the whole community and increase the potential stakeholders' incentives to join the MyData industry is a big consideration contributing to the successful initiative of the Financial MyData platform. The benefit and profitability guarantee mechanism may include a suitable revenue model for each participant, the possibility to develop more add-value services which has high chances to generate profit in the near future, and a fair compensation rate for data providers.

Finally, based on the role and number of state agencies and related organizations that are expected to participate, establish, and monitor the Financial MyData platform, assigning the missions and responsibilities for each involved participant is also considered a significant challenge. Defining and assigning roles for each participant may determine the success of the Financial MyData platform since it will fully regulate all the potential issues associated with personal data protection and utilization without any fragmentation of authority and overlapping functions in state management. For example, regarding the implementation practices of Korea, the Financial MyData platform can not be successfully implemented without the presence of FSC, FSS, and PIPC[24] as regulators and supervisory agencies, KCIS as the MyData Support

24) Personal Information Protection Commission

Center (including data relay service), and FSI as an organization in charge of technology standard setting, technical security support, and the integrated authentication relay system operating. Without a well-coordinated development roadmap, these structural mismatches and stakeholder misalignments could significantly hinder the effectiveness and scalability of a Financial MyData platform in Vietnam.

From the perspective of other participants involved in establishing the Financial MyData platform (e.g., financial institutions as data providers, private credit bureaus, and fintech companies as potential MyData operators), developing and updating the IT infrastructure to ensure data security for the data management system inside each organization is a considerable challenge. According to the annual financial statements of listed commercial banks, the year 2024 marked a significant leap in technology investment within Vietnam's banking sector, with total technology spending reaching VND 32,437 billion, equivalent to US$1.25 billion, accounting for 14.85% of the industry's total operating expenses. This is the highest proportion recorded in the past four years, reflecting a clear shift in the strategic mindset of financial institutions. Whereas banks were previously cautious about allocating budgets for technology due to cost barriers and implementation risks, digital transformation has emerged as a critical driver for improving productivity, optimizing costs, and safeguarding market share. According to the Vietnam Innovation & Tech Investment Report 2024, between 2013 and 2023, Vietnam's payment FinTech startups attracted a total of US$1.04 billion in investment, while an additional US$495 million was invested in financial services. In the context of stricter personal data protection regulations, greater investment in capital and high-quality human resources may be required to ensure effective compliance.

Additionally, another challenge to consider is the requirement to increase financial education and social responsibility, reducing the risk of moral hazard since employees in each organization involved are aware of the importance of regulations related to personal data protection. As long as employees clearly understand their responsibilities and the legal consequences of mishandling personal data, they are more likely to act following ethical standards and institutional policies. Regular training sessions and compliance workshops can help reinforce a culture of accountability and transparency across all levels of the organization. However, this issue remains underestimated in Vietnam. Numerous violations of legal regulations on personal data protection have originated from the wrongful actions or lack of awareness among employees or staff of some financial institutions or companies involved in collecting and processing personal data. So, embedding data protection principles into internal performance evaluations and risk management frameworks is needed to incentivize proper behavior. Over time, this strengthens the institution's internal control environment and enhances public trust in financial institutions' ability to manage personal data securely and responsibly.

3.1.4 The Governance Model Needs

As Vietnam considers the establishment of a Financial MyData platform, a comprehensive governance model must be proposed to ensure transparency, accountability, and consumer trust. Unlike conventional data-sharing systems, the MyData model requires multidimensional coordination between regulatory authorities, financial institutions, technology providers, and consumers. Governance in this context extends beyond legal compliance; it encompasses infrastructure

readiness, standardized consent mechanisms, institutional roles, and public supervision. A sound governance framework should not only facilitate secure data flows but also clearly define the rights and responsibilities of each stakeholder in the ecosystem.

Korea's official launch of the Financial MyData initiative in 2022, following careful regulatory preparations and inter-agency coordination, offers essential lessons for Vietnam. The Financial Services Commission (FSC) took a central role there, with regulatory support from the Personal Information Protection Commission (PIPC) and technical infrastructure built around the Open API framework. For Vietnam, applying this model with a proper adjustment to fit the current situation of Vietnam's landscape requires early institutional alignment and regulatory harmonization, particularly across the State Bank of Vietnam (SBV), the Ministry of Science and Technology (MST), and the Ministry of Public Security (MPS). These agencies must jointly ensure that governance regulations support data portability, consent traceability, cybersecurity, and equitable access. With these foundations, Vietnam can develop a governance system that enables a secure and competitive data economy, centered on consumer empowerment. The following requirements outline three core components essential to that governance model.

The first pillar of the governance model should be developing an integrated system that enables financial consumers to manage and control their data across all financial service providers. In Korea, the integrated platform facilitated this function by allowing users to view and manage their accounts, transactions, and credit data across multiple banks, insurers, and fintech firms. This integration was achieved through standardized APIs, supported by national digital infrastructure and monitored by the FSC. Vietnam must similarly build

an interoperable data system that allows seamless connection among banks, non-bank financial institutions, credit bureaus, and third-party processors. The system should ensure data is shared under unified technical and procedural standards, reducing fragmentation and enhancing data reliability. Centralized dashboards or mobile applications should be introduced to allow individuals to access consolidated information on their financial status, aiding in informed financial decisions. In addition, data access logs should be required by law to record when and by whom data is accessed or transferred. This enables effective audit mechanisms and strengthens consumer control. Such infrastructure will also support the growth of digital financial services by allowing new entrants to access verified data streams securely and in a regulated manner. However, the design and implementation of this system must involve broad consultation with financial institutions and technology developers to ensure operational feasibility. Legislative and technical coordination will be critical to prevent data silos and to promote equity among all data stakeholders.

The second component of the governance model is creating a standardized consent management system, enabling users to give or withdraw permission regarding their data usage. This system must provide transparency by clearly informing individuals when, where, and how their data is processed, transferred, and stored. Korea addressed this by amendment of its Credit Information Use and Protection Act, which required MyData service providers to obtain explicit, time-limited, and purpose-specific user consent. Consent records are digitally stored; users can modify or revoke them in real-time via mobile applications. In Vietnam, a similar system must be supported by clear legal definitions of consent, following the framework already partially outlined in PDPL. However, current enforcement and interoperability

mechanisms for consent across financial institutions remain limited. Therefore, the governance framework should designate a lead agency, such as the MST for the long-term consideration or the SBV for the short-term consideration, focusing on the Financial MyData platform initiative, to oversee the design and rollout of a unified consent architecture. This system should also include visual dashboards for users to track their consent history and receive alerts about third-party data sharing.

Furthermore, consent transactions should be logged in secure and immutable formats to prevent unauthorized changes or disputes. Consumer financial education campaigns will be necessary to raise public awareness and improve digital literacy on data rights. Overall, the success of this component depends on its integration with the broader regulatory and technical systems, ensuring legal enforceability and system reliability across platforms.

The third critical component of the governance model is the systematic assessment of current legal and regulatory frameworks to determine their adequacy in supporting a Financial MyData platform. Korea's MyData initiative was preceded by several years of legal reform, including revisions to its Personal Information Protection Act and new licensing criteria for MyData operators. These legal updates provided the necessary clarity and institutional confidence for data sharing. In Vietnam, while specific laws such as the Law on Cybersecurity (2018), Law on Credit Institutions (2010, amended), and the recently issued PDPL provide partial guidance, no unified legal framework exists for financial data mobility. Regulatory fragmentation poses a significant obstacle, with overlapping mandates among agencies and conflicting data retention, consent, and cross-border transfers provisions. A comprehensive legal impact assessment should be

conducted to identify gaps, redundancies, and inconsistencies within the current legislative environment. Based on this assessment, Vietnam can determine whether new laws or amendments are necessary to establish legal certainty and safeguard consumer rights. Importantly, this process must be transparent, inclusive, and consultative, involving all key stakeholders, including financial service providers, consumer groups, legal experts, and government bodies. Lessons from Korea show that MyData platforms may face regulatory bottlenecks that undermine their scalability and trustworthiness without early legal harmonization. Therefore, legal readiness must not be treated as a secondary task but as a foundational element in the governance roadmap for Vietnam's financial data ecosystem.

3.2 Comparative Analysis with Korea

3.2.1 Opportunities for Adaptation

a. Similarities and differences of the MyData platform established by Korea with other successful models or international standards.

Thanks to the diversity of financial service providers in Korea's financial ecosystem, the financial market in Korea illustrates its dynamic and agile environment that facilitates all participants' activities, targeting financial consumers' benefits and financial institutions' profitability. The development and upsurge of the MyData industry in Korea is inevitable when the country puts much effort into focusing on human-centric data management. Currently, the MyData platform, which is developed and operated in Korea, is fostered with well-regulated legislation

Figure 4. Similarities Regarding Some Aspects Facilitating the MyData Platform Development

Aspect	Korea (MyData)	UK	Singapore	EU Countries
User-Centric Data Portability	Individuals have the right to retrieve and transfer their personal data from data holders to licensed MyData operators.	The UK implemented data portability rights under Article 20 of the UK GDPR and the Data Protection Act 2018, allowing individuals to receive and transfer their own personal data under specific conditions.	The Amendment PDPA has introduced a Data Portability obligation, which is set out in Part 6B of the PDPA. However, it has yet to come into effect.	GDPR Article 20 provides a legal right to personal data portability across any controller, using structured, machine-readable formats
Purpose-Limited Data Use	Data collected must be used only for the purposes consented to by the individual. The consent need to be renewed yearly. Reuse or secondary use without permission is prohibited.	Article 5(1)(b) of UK GDPR Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…	Section 13 of the PDPA[25] requires organizations to obtain consent and use data only for appropriate and disclosed purposes.	GDPR Articles 5(1)(b) and 6 define purpose limitation and lawful basis for data processing. **Australia** – CDR Rules (Part 7) enforce consent-based data use, and prohibit use beyond the scope of the consumer's agreement.
Standardized APIs	Use of Open API infrastructure mandated by government-led standards.	Standardized APIs are mandated under the Open Banking regime, which was introduced by the Competition & Markets Authority (CMA) in 2016 and enforced from January 2018. These APIs allow secure, interoperable, and consent-based sharing of customer banking data between financial institutions and third-party providers.	SGFinDex[26] is built on interoperable APIs developed and maintained by GovTech (Government Technology Agency) and operates under the regulatory oversight of both MAS (Monetary Authority of Singapore) and PDPC (Personal Data Protection Commission).	PSD2 (Revised Payment Services Directive, effective January 2018) mandates that banks (ASPSPs) provide secure, API-based access to customer account and payment data to authorized third-party providers (TPPs) when consent is given — facilitating data portability via account information (AIS) and payment initiation (PIS) services. Berlin Group NextGenPSD2 offers a harmonized pan-EU API framework.
Consent Management	Explicit, purpose-bound, and revocable consent is required. Consent history must be trackable.	Consent for personal data sharing and portability is governed by two primary frameworks: Articles 6-7 and 20 of the UK GDPR (post-Brexit GDPR adaptation) and Open Banking Framework which is mandated by the CMA Order 2017 and supervised by the FCA under PSD2[27]	PDPA mandates clear, documented consent and allows individuals to withdraw consent at any time.	GDPR Articles 6-7 require informed, specific, and revocable consent, with clear accountability
Centralized Oversight Body	FSC and PIPC (Personal Information Protection Commission) jointly supervise MyData.	Information Commissioner's Office (ICO) has responsibilites including enforcement of personal data protection across all sectors (public and private), oversight of data subject rights (e.g., access, correction, erasure, portability under Article 20), and guidance on consent management, lawful processing, privacy notices.	Monetary Authority of Singapore (MAS) regulates financial activities, while Personal Data Protection Commission (PDPC) enforces personal data protection laws.	Each member state appoints a national Data Protection Authority (DPA), coordinated under the European Data Protection Board (EDPB).

Source: Data compiled from various sources

25) Personal Data Protection Act

26) SGFinDex is the Singapore's digital infrastructure linking the various data sources from participating entities to facilitate the sharing of personal financial information. With such convenient linkages, financial consumers will be able to securely retrieve their personal financial data from their selected data sources and have a consolidated view of their personal financial position through their preferred participating financial planning applications/websites. GovTech created the API infrastructure, known as SGFinDex

Figure 5. Differences Regarding Some Aspects Facilitating the MyData Platform Development

Aspect	Korea (MyData)	UK	Singapore
Name of platform	MyData	MiData	SGFinDex
Regulatory Licensing Scheme	A Credit Information Company including MyData operators must be licensed by the Financial Services Commission (FSC) *(Credit Information Use And Protection Act, Article 4).*	Not applied for MyData operators. But there are some specific requirements on related licensing scheme to enhance data protection. AISPs[28]and PISPs[29] are licensed under PSD2 and regulated by the Financial Conduct Authority (FCA). Compliance includes operational resilience, safeguarding, and customer protections (FCA Handbook).	Not applied for MyData operators.
Scope of Sectoral Coverage	Primarily focused on financial sector initially (Financial MyData) and now attempt to extend with health record data, public data, telecom data and education data.	The Midata pilot targeted four key consumer sectors: banking, energy, telecommunication, utilities & loyalty.	SGFinDex Sectoral Coverage: bank-related data (account balances, deposits, savings, loans, and credit card information), investment data, (holdings and securities information), data from government financial agencies (taxable income, housing loans, retirement savings data and relevant financial data), and insurance data.
Data Flow Architecture	Primarily **one-way** from data providers to MyData operators	**Two-way APIs** between banks and authorized TPPs (under PSD2)	**Pull-based,** user-initiated one-way flows with periodic consent
Cross-Border Data Portability	Restricted (cross-border transfer heavily limited under privacy laws)	Allowed under GDPR/UK GDPR with safeguards; limited in practice	Not supported by SGFinDex; domestic use only
Identity Verification Integration	Strong national systems: i-PIN, Mobile Authentication (PASS, Kakao, Naver, Toss), Digital Certificates.	OAuth 2.0 + OpenID in Open Banking; no unified national ID system	Integrated with SingPass (National Digital Identity)
Government-Initiated Development	FSC and PIPC led legal reforms, licensing, infrastructure	The Competition and Markets Authority CMA played a pivotal role in initiating the Midata pilot, particularly within the energy sector. Information Commissioner's Office (ICO) did not directly regulate the pilot, it provided crucial guidance and oversight regarding data privacy, consent	Led by Monetary Authority of Singapore (MAS) with GovTech support

APIs, which utilize OAuth 2.0 and OpenAPI machine-readable formats to enable consent-based data retrieval and interoperability across participating banks and government agencies

27) Revised Payment Services Directive

Aspect	Korea (MyData)	UK	Singapore
		frameworks, and data portability best practices under the Data Protection Act.	
Development Speed	Fast: Starting from 2018, legal revision in 2020; full launch in 2022	Medium: The voluntary pilot ran from late 2011 through at least 2014. The energy sector pilot paused around 2022.	Fast: SGFinDex launched ~2020; expanded with MAS coordination
Revenue Model	MyData operators monetize value-added services (e.g. credit insights, financial planning, commissions from promoting financial products, subcription fees for advanced features, advertising, cross-selling financial products)	Open Banking providers operate under cost recovery or freemium; monetization still constrained by regulation	SGFinDex infrastructure is state-funded and free for end-users. However, banks/insurers can monetize with value-added features (portfolio analytics, net-worth tracking, and financial advice, which could be monetized through subscription models or advisory fees)
Current Status	Continuous development with the expandation in the number of API transactions and MyData subcribers	Stopped since 2022 (energy sector) and since 2014 (remaining sectors)	Continuous development of SGFinDex with expanding coverage

Source: Data compiled from various sources

28) Account Information Service Providers

29) Payment Initiation Service Providers

related to data protection, similar to some areas or countries having strict regulations on data protection and utilization. The tables below show similarities and differences between the MyData platform operated in Korea and those in other countries and specific areas.

Based on the following analysis, Korea's MyData industry has exhibited a markedly higher level of development than several other countries that have introduced or are operating similar platforms. This is particularly evident in its effective balance between safeguarding personal data and enhancing the benefits available to stakeholders, most notably in terms of data subject control rights and the capacity to generate value and profit from data.

Supported by a robust and adaptable legal framework for personal data protection, closely aligned with the regulatory standards of the European Union, Singapore, and the United Kingdom, Korea's MyData initiative continues to advance, progressively expanding the scope and integration of financial data. This legal and institutional foundation creates favorable conditions for financial consumers to access a comprehensive and accurate view of their financial information, thereby facilitating more informed, data-driven decision-making in the context of financial services.

An examination of Korea's MyData implementation experience and the notable similarities in financial infrastructure between Korea and Vietnam suggests that Vietnam has significant potential to develop a comparable MyData platform, focusing on the Financial MyData platform. Such an initiative would serve not only as a practical mechanism for exercising data subject rights under national legislation but also as a catalyst for responsible innovation and the broader utilization of personal data within the financial ecosystem.

b. Comparative analysis of the encouraged conditions to facilitate the possibility of establishing the MyData platform in Korea and Vietnam

Similarity in financial infrastructure

Both Korea and Vietnam operate under centralized regulatory systems, where the central bank plays a pivotal role in supervising the banking and financial services sector. In Korea, the Bank of Korea (BOK) oversees monetary policy, while the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS) handle regulatory oversight of banks and financial institutions. In Vietnam, the State Bank of Vietnam (SBV) functions both as the central bank and the key regulator for monetary policy, banking operations, and financial stability.

The banking system structure in Vietnam and Korea also has some similarities. Both countries feature a tiered banking structure, where state-owned and private commercial banks dominate retail banking and credit markets. Regarding the credit information sector, Vietnam and Korea are both chasing the model of a proactive and competitive ecosystem with the national-level credit registry and private credit bureaus, in which the credit registry takes responsibility to support state management functions, and the private credit bureau operates to enhance financial access and risk management across banking systems. In addition, the diversity of financial participants is a prominent similarity, which represents the active financial ecosystem with a diverse mix of banks, fintech firms, insurers, and non-bank credit institutions (including consumer finance companies, e-wallet operators, peer-to-peer lenders, buy now pay later service providers).

The possibility of promoting MyData industry with the Financial MyData Initiative operated within the banking system.

The Financial MyData Initiative has successfully promoted Korea's MyData industry. With the coherent development stage (direct inquiry, direct inquiry and store, request to transfer data to a third party, one-stop inquiry to multiple companies, and control over all of my data), Korea prudently implements a step-by-step development for each sector, starting with financial sector and broadening with public sector, telecommunication sector and medical sector. An increasing number of MyData service subscribers and accumulated API transfers illustrate the success and potential of the MyData platform in facilitating secure and consumer-centric data exchange.

In Vietnam, the operational framework governing the credit information sector distinguishes between public credit registries and private credit bureaus, with each type of credit information service provider (CISP) subject to a separate regulatory instrument. The activities of private credit bureaus are regulated under Decree No. 58/2021/ND-CP, dated June 10, 2021, issued by the Government of Vietnam, which provides the legal basis for providing credit information services. In contrast, the operations of the public credit registry are governed by Circular No. 15/2023/TT-NHNN, dated December 5, 2023, issued by the State Bank of Vietnam (SBV), which sets out specific provisions related to the SBV's credit information activities.

Thanks to its capacity in policy formulation and implementation supervision, similar to FSC and FSS, the SBV is well-positioned to propose amendments to the current regulatory framework governing its credit information operations. Such revisions would support the development of the Financial MyData platform. Furthermore, the SBV can coordinate with other ministries and relevant stakeholders to facilitate the expansion of the Financial MyData initiative beyond the financial sector, promoting broader data integration and cross-sectoral

application.

The advantage of the current project about the shared specialized database in the banking system

Vietnam's banking sector is undergoing a rapid transformation marked by the widespread adoption of digital transaction channels. According to data from the State Bank of Vietnam (SBV), approximately 90% of transactions at many credit institutions are now conducted through digital platforms, and over 87% of the adult population holds a bank account. A broad range of banking services, including deposits, account opening, card issuance, money transfers, and lending, has been fully digitized, significantly reducing processing time and operational costs while enhancing overall customer convenience.

Data has emerged as a vital asset in the banking sector, playing a dual role in facilitating digital transformation and informing data-driven policymaking. The availability of accurate and timely data supports more effective and responsive policy development, contributing to improved governance and financial inclusion.

In this context, the SBV officially launched the "Assessment of the current status of the shared specialized banking database" project in April 2025. Funded by the World Bank (WB) and the Swiss State Secretariat for Economic Affairs (SECO), the project aims to design and implement an integrated data system that supports end-to-end data governance, from collection and processing to analysis and sharing, utilizing modern technologies and big data infrastructure. The system is being developed with an emphasis on scalability, flexibility, and interoperability with databases managed by other ministries, sectors, and national platforms under Vietnam's broader digital government initiative. Notably, data standardization is a central component of the

project. Thus, it is possibly regarded as a foundational condition for the potential exploration and development of a MyData platform within Vietnam's financial sector.

3.2.2 Identify the Potential Key Players Involved and the Proposed Operational Structure for Establishing the Financial MyData Platform in Vietnam

Based on the current assigned functions and duties of each potential participant in Vietnam's financial infrastructure, the likely key players regarding the two functions, including governing the operation of the Financial MyData platform and operating the Financial MyData platform, are as follows:

1) Financial MyData platform: Potential regulators

- **The State Bank of Vietnam (SBV):** The ministry-level agency is responsible for designing and proposing a suitable legal framework to facilitate the Financial MyData Platform by amending the current regulations related to credit information activities for the public and private sectors.
- **The Department of System Safety Supervision of Credit Institutions:** The state management agency operates under the SBV's regulation and oversees the stability, safety, and prudential performance of the banking and credit institution system in Vietnam. It operates based on legal mandates outlined in the Law on Credit Institutions, inspection laws, and specific SBV regulations (including data protection-related regulations).
- **A newly established agency:** It is an independent authority tasked

with overseeing data protection laws, regulating personal data handling, and resolving consumer complaints or disputes related to data protection on a cross-sectional scale. Its role is similar to that of PIPC (Korea) and PDPC (Singapore). Although The Department of Cybersecurity and High-Tech Crime Prevention (A05) has been assigned as the state management agency in charge of the data protection affairs by the current regulation, an independent authority with functions similar to PIPC and PDPC is essential for guaranteeing neutrality, fairness, and transparency in how personal data is collected, processed, and shared across MyData platforms.

2) Financial MyData platform: Potential core participants

- **Financial Consumers (Data subjects):** A financial consumer is any individual who uses financial services and whose personal financial information is collected, held, or transmitted under the MyData business model.
- **Data Providers:** A data provider is a financial institution or related entity (e.g., banks, card companies, fintech companies with lending activities such as BNPL, P2P lending) that holds personal financial data and is legally obligated to transfer such data to licensed MyData operators upon user consent.
- **MyData Operators:** A MyData Operator is an accredited or licensed entity that receives personal data from data providers (e.g., banks, government agencies) based on the data subject's consent and offers value-added services (e.g., financial planning, credit analysis, or data visualization) to the individual. These operators are a core component of the MyData ecosystem, functioning as intermediaries between data subjects and data

providers under a regulated framework. The number of MyData Operators should be prudently considered to fit the market size and avoid the risk of market saturation and fragmentation.

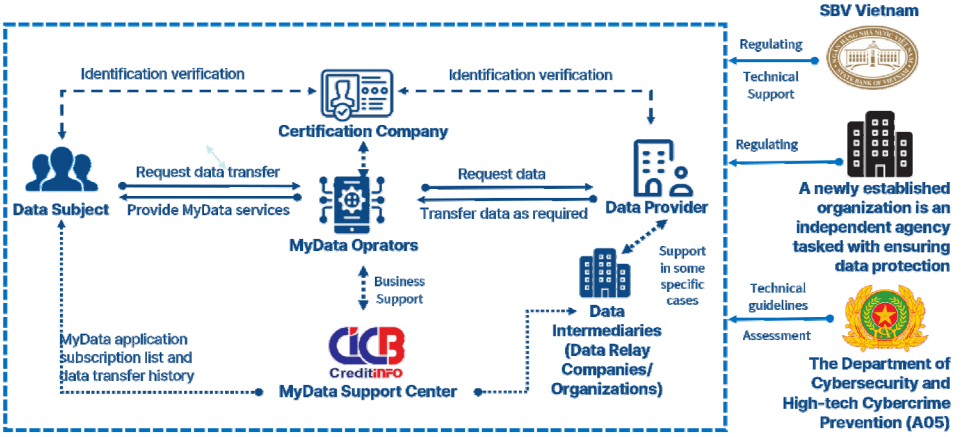
- **Certification companies:** A certification company is a trusted third-party service provider that offers secure user authentication, identity verification, and digital certificate issuance to ensure that the legitimate data subject initiates data access or transfer requests. These companies are critical in enabling secure and legally compliant data sharing between individuals, data providers, and MyData operators, particularly where digital identity and user consent must be authenticated. About 14 Fintech companies currently provide eKYC solutions, some of which are funded or are subsidiaries of big tech companies such as FPT and VNPT. However, certification companies should meet specific requirements regulated by a relevant state authority to participate in the MyData industry.
- **Key Data Intermediaries (Data Relay Companies/Organizations to ensure and support secure data flow):** Key Data Intermediaries are specialized entities (both public and private organizations) that act as technical and operational bridges between data providers and data recipients (e.g., MyData Operators), ensuring that personal data is transmitted securely, accurately, and with the appropriate consent of the data subject. They are responsible for standardizing, encrypting, and routing personal data flows while enforcing legal and cybersecurity protocols. In Vietnam's banking sector, there are approximately 1.640 People's Credit Funds across 34 cities/provinces, operating to support mutual development and improve livelihoods through financial services. Due to their limited operational scale, some People's Credit Funds cannot invest in

modern information technology infrastructure. As a result, the role of Key Data Intermediaries becomes essential in supporting and advancing the implementation of the Financial MyData platform in Vietnam. To ensure the platform's sustainable and continuous operation upon its official launch, it is necessary to identify capable and appropriate data intermediaries and formally assign them responsibilities within the system architecture.

- **The Department of Cybersecurity and High-Tech Crime Prevention (A05):** A state management agency under the Ministry of Public Security (MPS), tasked primarily with ensuring cybersecurity and safety, as well as implementing measures for the prevention, detection, investigation, and handling of crimes involving the use of high technology. A05's role is similar to that of FSI in developing security guidelines, conducting vulnerability assessments, and providing technical support for participants involved.
- **The National Credit Information Centre of Vietnam (CIC Vietnam):** the unique public credit registry operates under the regulation and management of the SBV. It serves as the vital data infrastructure behind Vietnam's credit market. It enables better risk management, transparency, and policy support by providing credit reports and other value-added services for better data-driven decision making. Thus, CIC Vietnam can be a MyData support center like KCIS due to its infrastructure, regulatory mandate, and neutral position in supporting safe, standardized, and equitable financial data sharing.

The proposed operational structure is illustrated in the following diagram.

Figure 6. The Proposed Operational Structure of the Financial MyData Platform



3.2.3 Institutional and Policy Gaps

Based on the analysis of the maturity and readiness of the current legal framework regarding data protection to facilitate the development of the Financial MyData platform, institutional and policy gaps can be identified as shown in the table below. The analyzed dimension includes: Legal Right to Data Portability; Lead Data Governance Body; Data Dictionary / Taxonomy; Open API Specifications; Standard Consent Framework; Centralized API Gateway (Hub); Data Quality Management; Security Oversight & Certification; Consumer Awareness & Trust.

The gap analysis highlighted critical challenges Vietnam must address to successfully develop a Financial MyData platform aligned with global best practices. Unlike South Korea, the UK, Singapore, and the EU, Vietnam has not yet enacted a legal right to data portability; this absence represents a foundational obstacle and must be urgently rectified. Governance remains fragmented among ministries without a centralized and independent authority, unlike countries with clear, empowered regulators like the PIPC in Korea or the PDPC in Singapore.

Vietnam also lacks a standardized data taxonomy and mandated API specifications, essential for interoperability and secure data exchange. The consent framework varies by service, while other countries provide unified dashboards and granular control mechanisms. Data quality and cybersecurity oversight are also weak in Vietnam, with no formal audit standards or certification programs, creating risks for consumers and service providers. While SBV operates a centralized API system for banking, there is no national API gateway for cross-sector data sharing like Singapore's SGFinDex. Compared to robust public engagement strategies in Korea and Singapore, consumer trust is low due to limited awareness and frequent breaches. Overall, Vietnam faces high gaps in most critical dimensions and must prioritize legal reform, standardization, security, and public communication. Addressing these priorities will determine the feasibility and success of implementing a user-centric, secure, and scalable MyData platform.

Figure 7. Vietnam vs. Global Best Practices: Gap Analysis

Dimension	Vietnam (2025)	South Korea	UK	Singapore	EU	Gap	Priority
Legal Right to Data Portability	Not yet enacted across sectors	Financial portability under PIPA, CIUPA	Data portability right under UK GDPR Article 20 + PSD2 for banking	The Amendment PDPA has introduced a Data Portability obligation, which is set out in Part 6B of the PDPA.	GDPR Article 20 provides cross-sector portability	High	High
Lead Data Governance Body	Fragmented (MPS, Ministries, Ministry-level state authority)	FSC, PIPC	ICO	PDPC enforces PDPA; MAS regulates financial data access and SGFinDex	National DPAs coordinated under EDPB[30]	High	Medium
Data Dictionary / Taxonomy	Bank-specific formats. But SBV official launced new project related to data standardization	Standardized via FSC MyData APIs	OBIE common banking taxonomy	SGFinDex API uses GovTech-defined standardized data model for financial data aggregation	PSD2/CDR and standards like Berlin Group ensure consistent data schemas	Medium	High
Open API Specifications	No mandated API specifications	MyData requires mandatory RESTful APIs standardized by the FSC	Open Banking mandates RESTful APIs (FAPI-compliant, OAuth 2.0)	SGFinDex uses RESTful APIs with OAuth2 via SingPass for authentication	RESTful APIs mandated by PSD2 and CDR	High	High
Standard Consent Framework	Varies with service	MyData dashboard-based OAuth2 consent	OAuth2 consent with dashboard, Smart Data planned	Consent via SingPass gateway with explicit scopes and revocation capability	GDPR requires granular and revocable consent	Medium – High	High

30) the European Data Protection Board (EDPB).

Dimension	Vietnam (2025)	South Korea	UK	Singapore	EU	Gap	Priority
Centralized API Gateway (Hub)	Not available for national centralized API gateway. However, the Department of Information Technology of the SBV operates the centralized API gateway for the banking system.	No national centralized API Gateway (Hub) for MyData industry. However, some Data Relay Companies, such as KCIS, Koscom, KFTC act as centralized API hubs for specific groups of data providers.	Decentralized via OBIE	SGFinDex operates a central API gateway/hub developed by MAS and GovTech, enabling unified, centralized data relay via SingPass authentication.	PSD2 gateways are per-bank; no EU-wide hub	Medium	Medium
Data Quality Management	No national standards	FSC mandates validation and consistency audits	FCA audits data accuracy; CMA oversight via OBIE	SGFinDex enforces API validation – liability on providers for accuracy	PSD2 and CDR require verification thresholds and reconciliation	High	High
Security Oversight & Certification	No formal cybersecurity audit mandate for APIs	FSC mandates FSI, with MyData providers audited	FCA/PSR cybersecurity reviews for TPPs	MAS-certified infrastructure, Singapore CA integration, periodic security reviews	PSD2 SCA, ECB/EBA guidelines, NCA audits	High	High
Consumer Awareness & Trust	Low; unclear rules and limited public information	Medium-High; rising trust via PIPC and FSC campaigns	Medium-High; Open Banking adoption increasing, ICO oversight	High; SGFinDex trust reinforced by SingPass central identity, bold public outreach	Medium-High; GDPR promotion and sectoral consumer programs	Medium	Medium

Source: Data compiled from various sources

3.3 Policy Recommendations and Implementation Pathway

Although the legal regulations related to data protection and other related sub-level regulations to promote the introduction of the MyData service in Vietnam have a strong foundation, they are gradually closer to the international benchmark. However, some existing legal gaps highlight the need for a comprehensive strategy to strengthen Vietnam's regulatory framework and ensure effective enforcement mechanisms. Drawing on advanced models such as the EU's GDPR, Korea's PIPA, and Singapore's PDPC, the study puts forward several recommendations for improving the legal system as follows:

a. Clarify and expand provisions on data subject rights

As discussed above, one of the primary shortcomings of Vietnam's current legal framework is the lack of explicit provisions regarding data subject rights, particularly the right to data portability. The GDPR recognizes this right as fundamental, enabling individuals to transfer personal data to another service provider. In Vietnam, this right remains insufficiently codified, limiting users' ability to control their personal information in the digital environment.

In the scope of the financial and banking sector, to facilitate the establishment of the Financial MyData platform, it is therefore recommended that the credit information-related regulation formalizes the provision similar to the right to data portability, obligating online service providers to implement secure, convenient, and interoperable mechanisms for individuals to export and transfer their data to other

platforms. The credit information-related legal regulations for both the public and private sectors should be integrated into a single regulation regulated by the Vietnamese Government. The pilot result of the Financial MyData Platform can be used as an incentive to propose the right of data portability formalized in a higher level of legal regulation (e.g., PDPL and Data Law issued by the National Assembly of Vietnam).

b. Clearly define the mandates of data protection authorities and stakeholders involved in the MyData service

Clearly defining data protection authorities' mandates and institutional responsibilities is critical to enhancing enforcement. At present, Vietnam's personal data protection oversight is primarily assigned to the Department of Cybersecurity and High-Tech Crime Prevention (A05) under the Ministry of Public Security. This structure presents risks of potential conflicts of interest, especially in matters involving state data, and the fragmented authority across multiple agencies has hindered effective supervision and dispute resolution.

Accordingly, it is recommended that the government consider establishing an independent personal data protection authority, modeled after the Data Protection Authorities (DPAs) in the EU, the Information Commissioner's Office (ICO) in the UK, or the Personal Data Protection Commission (PDPC) in Singapore. Such a dedicated and autonomous body would monitor compliance, address individual complaints, issue regulatory guidance, and keep pace with technological developments. It would also facilitate international cooperation to promote global alignment in personal data protection standards.

The roles and responsibilities of each stakeholder involved in the

Financial MyData platform and the specific requirements for potential participants entering the MyData service should be clearly identified in the legal regulation, as in the case of Korea. It will enhance the benefits and obligations of each participant and ensure the operation of the proposed Financial MyData platform without interruption.

c. Escalating the process of the project about the development of the shared specialized banking database

The SBV is now on the way to promoting data standardization in the banking sector, which is marked with the project funded by the World Bank (WB) named "Assessment of the Current State of the Shared Specialized Banking Database." This project has a strong linkage with establishing the Financial MyData Platform since it promotes the process of data standardization across the whole banking system. An expanded working group could be formed to discuss and solve related key issues, such as API specification, mechanisms to ensure business viability, the necessary number of MyData operators fitting with the current market size in Vietnam, etc.

d. Launch a limited-use pilot for the Financial MyData Platform

To effectively assess the feasibility of implementing a Financial MyData platform in Vietnam, initiating a limited-use pilot program under close regulatory oversight is essential. This pilot should involve a select group of three to five major financial institutions, including commercial banks, consumer finance companies, fintech firms participating in the regulatory sandbox, and a data intermediary such as the Credit Information Center (CIC) or the Department of Information

Technology of the State Bank of Vietnam (SBV).

The pilot program should concentrate on key functional areas such as account aggregation, credit information transfer, and consent-based data access, enabling a realistic evaluation of technical and legal readiness. Implementing standardized APIs and a robust consent management interface will be essential to ensure secure and user-controlled data flows.

Clearly defined roles and responsibilities must be assigned to data providers, MyData operators, and the supervisory authority to ensure compliance with legal requirements and facilitate coordinated incident response. In addition, key performance indicators (KPIs), including system stability, user experience, data security, and error rates, should be established to guide performance assessment.

The pilot will provide a valuable opportunity to identify and address regulatory gaps, such as the absence of an explicit legal right to data portability. It also offers a platform to collect stakeholder feedback, enhance institutional capacity, and promote consumer awareness regarding personal data rights and digital financial services.

By advancing through a controlled and well-monitored pilot phase, Vietnam can minimize systemic risks while laying a solid foundation for the nationwide rollout of the Financial MyData platform. This approach is consistent with international best practices, as demonstrated in countries such as South Korea and Singapore, where pilot initiatives have been pivotal in refining system design and policy frameworks.

Ⅳ Conclusion

The development and upsurge of the MyData industry in Korea is inevitable when the country puts much effort into focusing on human-centric data management through well-regulated legislation related to data protection. Sharing some significant similarities in financial infrastructure, the pathway of developing and fostering the MyData platform in Korea shows a valuable case study for many countries, including Vietnam, to promote data protection and escalate data utilization capacity, bringing benefits to the community.

References

Assets Publishing Service. (July 2014). Review of the midata voluntary programme: Revision 1. GOV.UK. Retrieved June 29, 2025, from https://assets.publishing.service.gov.uk/media/5a7ec945e5274a2e87db1e67/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf

Duarte, F. (2025, March 8). Amount of data created daily (2024). Exploding Topics. Retrieved June 29, 2025, from https://explodingtopics.com/blog/data-generated-per-day

Dharmaraj, S. (2025, January 25). Vietnam: A major player in the global tech landscape. OpenGov Asia. Retrieved June 29, 2025, from https://opengovasia.com/2025/01/25/vietnam-a-major-player-in-the-global-tech-landscape

Fintech News Singapore. (2024, May 22). Cashless Vietnam. Retrieved June 29, 2025, from https://fintechnews.sg/104283/vietnam/cashless-vietnam/

Gov.uk. (n.d.). GDS API technical and data standards. Retrieved June 29, 2025, from https://www.gov.uk/guidance/gds-api-technical-and-data-standards

Gov.uk. (n.d.). Make better use of data. Retrieved June 29, 2025, from https://www.gov.uk/guidance/make-better-use-of-data

Hoàng Quân. (February 2025). Triệt xóa ổ nhóm mua bán gần 56 triệu thông tin dữ liệu cá nhân. Công An. Retrieved June 29, 2025, from https://congan.com.vn/vu-an/phong-chong-toi-pham-tren-khong-gian-mang/triet-xoa-o-nhom-mua-ban-gan-56-trieu-thong-tin-du-lieu-ca-nhan_173874.html

Korea Capital Market Institute (KCMI). (2024). MyData and the financial data ecosystem in Korea. Retrieved June 29, 2025, from https://www.kcmi.re.kr/kcmifile/webzine_content/OPINION/6008/webzinepdf_6008.pdf

Ministry of Information and Communications. (n.d.). Vietnam's data center market is expected to reach US$12.6 billion by 2030. Retrieved June 29, 2025, from https://english.mic.gov.vn/vietnams-data-center-market-to-reach-us126-billion-by-2030-197240325154250333.htm

Mondaq. (2025, January 15). Circular 50 strengthens security for online banking in Vietnam. Retrieved June 29, 2025, from https://www.mondaq.com/financial-services/1569470/circular-50-strengthens-security-for-online-banking-in-vietnam

MyData Global. (2020). MyData white paper. Retrieved June 29, 2025, from https://mydata.org/wp-content/uploads/2020/08/mydata-white-paper-english-2020.pdf

National Development Council (Taiwan). (n.d.). Digital government. Retrieved June 29, 2025, from https://www.ndc.gov.tw/en/nc_8455_34364

Ofgem. (n.d.). Midata energy programme. Retrieved June 29, 2025, from https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/midata-energy-programme

Quản lý Nhà nước. (2025, February 13). Pháp luật về bảo vệ dữ liệu cá nhân tại ngân hàng ở Việt Nam: Thực trạng và giải pháp. Retrieved June 29, 2025, from https://www.quanlynhanuoc.vn/2025/02/13/phap-luat-ve-bao-ve-du-lieu-ca-nhan-tai-ngan-hang-o-viet-nam-thuc-trang-va-giai-phap/

Reimsbach-Kounatze, C. and A. Molnar (2024), "The impact of data portability on user empowerment, innovation, and competition", OECD Going Digital Toolkit Notes, No. 25, OECD Publishing, Paris, https://doi.org/10.1787/319f420f-en

Saigon Times. (2024). Các ngân hàng thương mại đang chi hàng chục ngàn tỉ đồng cho công nghệ. Retrieved June 29, 2025, from https://thesaigontimes.vn/cac-ngan-hang-thuong-mai-dang-chi-hang-chuc-ngan-ti-dong-cho-cong-nghe/

SGFinDex. (n.d.). API specifications for SGFinDex. Retrieved June 29, 2025, from https://specs.api.sgfindex.gov.sg/

SGFinDex. (n.d.). Singapore Financial Data Exchange. Retrieved

June 29, 2025, from https://www.sgfindex.gov.sg

Tạp chí Ngân hàng. (2024, March 15). Kết nối và chia sẻ dữ liệu thông qua nền tảng tích hợp chia sẻ dữ liệu quốc gia. Retrieved June 29, 2025, from https://tapchinganhang.gov.vn/ket-noi-va-chia-se-du-lieu-thong-qua-nen-tang-tich-hop-chia-se-du-lieu-quoc-gia-9535.html

Tạp chí Luật sư Việt Nam. (2024). Pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam: Những khoảng trống và hướng hoàn thiện. Retrieved June 29, 2025, from https://lsvn.vn/phap-luat-ve-bao-ve-du-lieu-ca-nhan-o-viet-nam-nhung-khoang-trong-va-huong-hoan-thien-a156811.html

TechReg. (2024). Data portability, data sharing, and user empowerment: Comparative insights. Retrieved June 29, 2025, from https://techreg.org/article/view/11539/14820

Thời báo Tài chính Việt Nam. (2024). WB hỗ trợ chuyển đổi số, chuẩn hóa hệ thống dữ liệu dùng chung cho ngành ngân hàng. Retrieved June 29, 2025, from https://thoibaotaichinhvietnam.vn/wb-ho-tro-chuyen-doi-so-chuan-hoa-he-thong-du-lieu-dung-chung-cho-nganh-ngan-hang-174114.html

Tran Thi Thanh Bich, Dao Thi Anh Thu (2025). Pháp luật về bảo vệ dữ liệu cá nhân ở Việt Nam, những khoảng trống và hướng hoàn thiện. Luật sư Việt Nam. Retrieved July 5, 2025, from https://lsvn.vn/phap-luat-ve-bao-ve-du-lieu-ca-nhan-o-viet-nam-nhung-khoang-trong-va-huong-hoan-thien-a156811.html

Tuổi Trẻ. (2023, June 20). Nhân viên ngân hàng bán thông tin tài khoản chỉ 200.000 đến 1,9 triệu/trường hợp. Tuổi Trẻ Online. Retrieved June 29, 2025, from https://tuoitre.vn/nhan-vien-ngan-hang-ban-thong-tin-tai-khoan-chi-200-000-den-1-9-trieu-truong-hop-20230619222706361.htm

Ủy ban Bảo vệ Thông tin Cá nhân Hàn Quốc (PIPC). (n.d.). Reporting personal data infringement. Retrieved June 29, 2025, from https://www.pipc.go.kr/eng/user/lgp/ntp/reportingInfringement.do

Ủy ban Bảo vệ Thông tin Cá nhân Hàn Quốc (PIPC). (n.d.).

Request access to personal information. Retrieved June 29, 2025, from https://www.pipc.go.kr/eng/user/lgp/ntp/requestAccess.do

Vietnam.acclime. (2024). Vietnam Fintech Brief 2024. Retrieved June 29, 2025, from https://vietnam.acclime.com/downloads/guides/Vietnam%20Fintech%20Brief%20-%202024.pdf

Vietnam News Business Association (VNBA). (2024). Khai thác dữ liệu – nâng cao hiệu quả điều hành hoạt động ngân hàng. Retrieved June 29, 2025, from https://vnba.org.vn/vi/khai-thac-du-lieu--nang-cao-hieu-qua-dieu-hanh-hoat-dong-ngan-hang-17230.htm

Vu, Q. M. (2025, January 15). Circular 50 strengthens security for online banking in Vietnam. Mondaq. Retrieved June 29, 2025, from https://www.mondaq.com/financial-services/1569470/circular-50-strengthens-security-for-online-banking-in-vietnam

Woori Mobile. (2024, November 14). Must-have Verification Apps in Korea. Retrieved June 29, 2025, from https://woorimobile.kr/article/k-culture/12/191/

Abstract

This research examines the legal and institutional prerequisites for developing a Financial MyData platform in Vietnam, with a particular focus on the regulatory role of the State Bank of Vietnam (SBV). Using a qualitative legal research approach, the paper analyzes Vietnam's current data protection-related legal regulations and other sub-level regulations and conducts a comparative review of international models, focusing on the successful model of MyData platform in Korea. Analyzing the maturity and readiness to establish the Financial MyData platform in Vietnam and conducting a comparative analysis about the supported elements for Vietnam's financial infrastructure, the research highlights key regulatory gaps, such as the absence of a formal right to data portability, data standardization, API specification framework, etc., and proposes a phased approach through a controlled pilot program. Findings suggest that while foundational elements exist, targeted legal reforms and institutional coordination are essential to enable secure, consent-based data sharing. The study offers policy recommendations for Vietnam to develop a modern and secure environment for better human-centric data governance.

Keywords: MyData platform, MyData service, human-centric data governance, data protection

Abbreviations

Abbr.	Full explaination
A05	The Department of Cybersecurity and High-Tech Crime Prevention
AISPs	Account Information Service Providers
API	Application Programming Interface
BNPL	Buy Now Pay Later
BOK	Bank of Korea
CIC	National Credit Information Centre of Vietnam
CISP	Credit Information Service Providers
CIUPA	Credit Information Use and Protection Act (Korea)
DPA	Data Protection Authority
DPDP	Decree No. 13/2023/ND-CP on Personal Data Protection (Vietnam)
DPIAs	Data Protection Impact Assessments
DRS	Data Subject Request
DTIAs	Data Transfer Impact Assessments
EDPB	European Data Protection Board
eKYC	Electronic Know Your Customer
EU	The European Union
FSS	Financial Supervisory Service (Korea)
FSI	Financial Security Institute (Korea)
FSC	Financial Services Commission (Korea)
GASA	Global Anti-Scam Alliance
GDPR	General Data Protection Regulation (EU)
GovTech	Government Technology Agency (Singapore)
ICO	Information Commissioner's Office
ICT	Information & Communications Technologies,
KCIS	Korean Credit Information Service (Korea)
KIF	Korea Institute of Finance (Korea)
LoCI	Law on Credit Institutions
LOCIS	Law on Cyber Information Security
LOCS	Law on Cybersecurity
MAS	Monetary Authority of Singapore
MPS	The Ministry of Public Security (Vietnam)
MST	The Ministry of Science and Technology (Vietnam)

Abbr.	Full explaination
OECD	The Organization for Economic Co-operation and Development
OTP	One time password
PCB	Private Credit Bureau
PCR	Public Credit Registry
PDPC	Personal Data Protection Commission
PDPL	Personal Data Protection Law (Vietnam)
PIPA	Personal Information Protection Act (Korea)
PIPC	Personal Information Protection Commission
PSD2	Revised Payment Services Directive
SBV	The State Bank of Vietnam
SECO	Swiss State Secretariat for Economic Affairs
TTPs	Third-party providers
UK	The United Kingdom

인 쇄 2025년 12월 24일

발 행 2025년 12월 29일

발행인 이항용

발행처 한국금융연구원

서울시 중구 명동 11길 19 은행회관 5·6·7·8층
전 화 : 02-3705-6300 FAX : 02-3705-6309
http://www.kif.re.kr ; webmaster@kif.re.kr
등록 제1-1838(1995. 1. 28)