CONSULTATION PAPER

Draft Regulation on Oversight of Mechanisms Enabling Customers to Exercise Their Right to Share Their Data Held by Financial Service Providers (Under the Your Data Project, within the purview of the Bank of Thailand)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Open Data for Consumer Empowerment is one of the key policies in the digital realm under Thailand's new financial landscape. Open Data will be a game changer leading to the development of digital financial innovations, enhancing service efficiency and better meeting customer needs, particularly (1) appropriate access to formal credit and (2) personalized financial management, especially for retail customers and small businesses, which remains a significant gap in the Thai financial system. Currently, customer data is scattered across various service providers and agencies. If there is a mechanism allowing customers to easily request their service providers and agencies to share their data to other service providers and agencies, in accordance with their rights under relevant laws, such as the Personal Data Protection Act, B.E. 2562 (PDPA), it will enable customers to better utilize their data to receive improved financial services.

The Bank of Thailand (BOT) and relevant agencies have collaborated on the Your Data initiative to create a digital mechanism empowering customer rights on their data stored at both financial and non-financial entities and utilizing such data for better access and financial services. For non-financial data, the BOT is working with the Digital Government Development Agency, relevant utilities agencies, and the Revenue Department to develop a channel enabling individuals to share their electricity and water usage and payment as well as tax-filing information with financial service providers, which is expected to be available by 2025. For financial data, the BOT is establishing mechanisms for customers of regulated financial service providers to digitally share their deposit, credit, and payment account information to other service providers. Additionally, the BOT is collaborating with the Securities and Exchange Commission (SEC) and the Office of Insurance Commission (OIC) to develop mechanisms enabling customers to also share their securities holdings and insurance policy data between financial service providers and those in the capital market and insurance sectors. To facilitate the implementation of mechanisms enabling customers to exercise their right to share their data held by service providers under the BOT's supervision, it is necessary to rely on (1) the establishment of rules and regulations to oversee service providers in creating digital data sharing mechanisms that are convenient, secure, and without undue restriction for customers to exercise their rights, and (2) the participation of relevant stakeholders in developing common standards and guidelines for data sharing to ensure practical implementation.

This document aims to gather feedback on the regulatory framework for service providers to establish mechanisms that allow customers to exercise their right to share their data held by financial service providers under the BOT's supervision, enhancing financial services to better meet customer needs, particularly in terms of appropriate access to credit and personalized financial management. The principles and key details are as follows:

1. Principles: Individuals as data owners have the right to request that the data collector share their data to other entities through automated means if the data collector has prepared the data in a machine-readable format and has an automated data sharing system in place to support the data owner's rights. Therefore, the BOT adopts the following principles in requiring its supervised service providers to establish mechanisms that enable customers to exercise their data portability right conveniently, securely, and without undue restriction.

1.1 The desired outcomes that the BOT wishes to see from such mechanisms are (green line): (1) Financial service providers holding significant customer data must prepare data and establish mechanisms that allow customers to conveniently exercise their right to share data through digital channels; (2) Service providers must be able to utilize the customer data received to develop and offer financial services that meet specific customer needs; (3) Data exchange between data providers and data consumers must adhere to established common standards and guidelines to ensure efficiency and avoid unnecessary burdens or costs.

1.2 Meanwhile, the following red line must not arise: (1) Conditions and fees are obstacles to service usage and data sharing, or there are excessive data requests or one-sided data transfers without reciprocal sharing; (2) Service providers have inadequate risk management, particularly regarding data security, data privacy, and consumer protection.

2. Key Details of the Regulation:

2.1 Scope of Financial Service Providers Required to Have a Mechanism that Enable Customers to Exercise Their Right to Share Their Data upon Customer Request (Data Provider): This must cover financial service providers that collect significant customer data, such as deposit, credit, and payment information, without imposing excessive costs on smaller providers or those with limited capability. The scope includes (1) financial

institutions and specialized financial institutions (SFIs) providing significant deposit services, meaning having a number of accounts exceeding a specified level (2) wide-coverage payment service providers with significant transaction volumes, such as e-money providers and credit card issuers, and (3) all regulated credit providers under the BOT's supervision, as retail customers and SMEs use loan services from both large and small providers.

2.2 Scope of Service Providers that can Receive Customer Data (Data Consumers): This must cover financial service providers capable of utilizing customer data to develop and offer services that better meet customer needs and are subject to appropriate data governance and security standards. This includes (1) financial service providers under the BOT's supervision, including financial institutions and SFIs (under the Financial Institution Business Act B.E. 2551), payment service providers and credit providers, and (2) other regulated service providers under similar regulatory regimes, initially focusing on those under the SEC and OIC. In the future, the scope could be expanded to include service providers in other sectors that meet similar regulatory standards.

2.3 Conditions and Fees Principles Related to Data Sharing: The principles for setting conditions and fees related to data portability must consider promoting the use of customer rights while avoiding unnecessary data sharing. Specifically, (1) conditions and processes should promote customer usage and greater data utilization, and (2) service providers must not impose conditions or fees that hinder data sharing or utilization, except in cases of excessive data requests where fees may be charged to discourage unnecessary requests.

2.4 Oversight of Consumer Protection and Data Sharing to Ensure Compliance with Common Standards and Security: The BOT will oversee service providers to ensure compliance with consumer protection, data privacy, and data sharing standards. This oversight aims to ensure customer confidence throughout the process to exercise their data sharing rights, without imposing excessive burdens on service providers or creating obstacles to data portability. This includes: (1) Consumer protection and data privacy, where service providers must comply with current laws such as the PDPA and additional relevant BOT regulations on consent, authentication, and authorization processes, ensuring clear communication of service terms to customers and convenient management of given consents and authorizations; (2) Data sharing according to common standards and

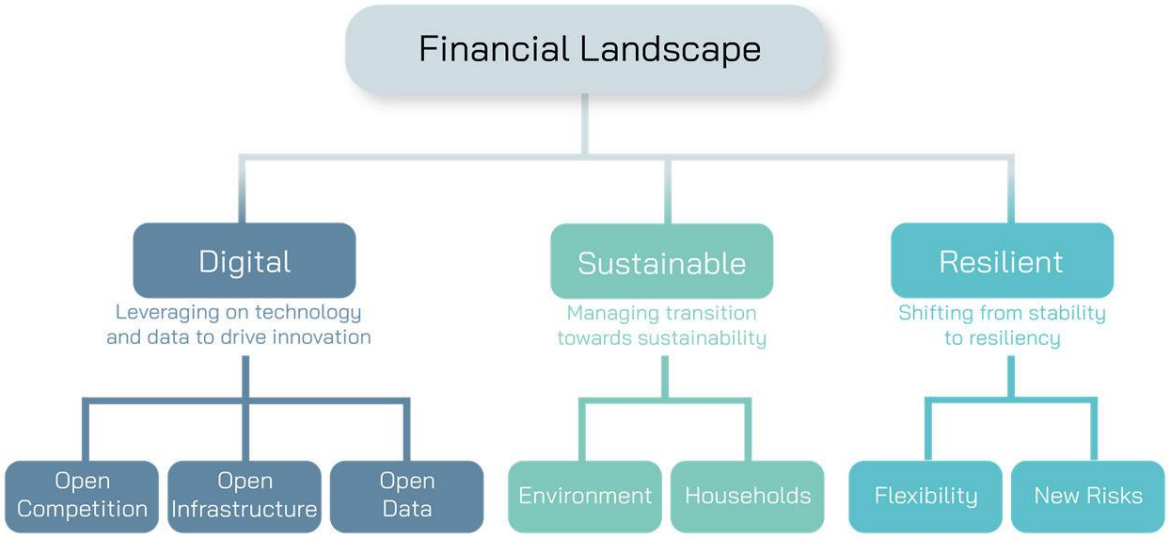
secure data management, where service providers must follow BOT standards and practices, ensuring data security and privacy throughout the process, including a good data governance by the board of directors and senior management, data security, and incident management.

2.5 Supervision Process to Ensure Service Providers' Compliance with Standards: The supervision process involves the BOT continuously overseeing data providers and data consumers to ensure compliance with this draft regulation. This includes: (1) Before starting data sharing services, service providers must pass compliance tests with common standards and guidelines. (2) During service provision, the BOT will continuously monitor and supervise service providers. If any issues or deficiencies in the system or services are found, the BOT can order the service providers to make corrections. (3) In the event of problems or disputes with customers, service providers must promptly report significant issues or incidents to the BOT. If the service provider is at fault or responsible for the issue, they must appropriately address, rectify, and compensate the customer, as well as implement measures to prevent recurrence.

2.6 Implementation Schedule: The BOT requires service providers to complete mechanisms for customers to exercise their data portability rights, starting with individual deposit account information within 6 quarters (which can leverage from existing standards) and individual loan and payment data within 7 quarters from the regulation's effective date (expected by Q4 2026 and Q1 2027, respectively). Juristic deposit, credit and payment account information must be ready within 9 and 10 quarters, respectively (expected by Q3 and Q4 2027), allowing more time for system development. In cases of reasonable necessity due to uncontrollable factors, service providers may request an extension from the BOT on a case-by-case basis, providing reasons, necessities, and relevant details.

1. INTRODUCTION

Open Data for Consumer Empowerment is one of the key policies in the digital realm under Thailand's new financial landscape.[1] This will allow the financial sector to leverage technology and data to develop innovations and financial services that better meet the needs of retail customers at a lower cost, while also demonstrating social responsibility (responsible innovation).



In the development of digital financial systems, beyond the introduction of the fast payment system like PromptPay as a game changer that has expedited and facilitated payments, data portability will be another crucial game changer driving the development of digital financial innovations. This will help enhance service efficiency and better meet the needs of users. Firstly, data portability will facilitate appropriate access to formal credit, particularly for non-salary individuals and small businesses with potential but thin-file financial history with financial institutions, who may possess other types of data from various sources. Secondly, data portability will enable personalized financial management for small businesses and individuals, allowing the consolidation of financial account information in a single place for further value-added services. Both use cases remain a significant gap in the Thai financial system.

[1] For more details on the new Thailand financial landscape, please refer to https://www.bot.or.th/content/dam/bot/financial-innovation/financial-landscape/ConsultationPaper-FinancialLandscape-EN.pdf"

However, customer data is currently scattered across various financial service providers and agencies. If there is a mechanism allowing customers to easily request their service providers and agencies to share their data to other service providers and agencies, in accordance with their rights under relevant laws e.g., the Personal Data Protection Act, B.E. 2562 (PDPA), it will enable customers to better utilize their data to receive improved financial services.

Many countries, including Singapore, the United Kingdom (UK), Australia, South Korea, India, and Brazil, have developed mechanisms allowing customers to exercise their right to share their data held by various service providers and agencies as stipulated by law. This primarily began with data from financial sectors, such as deposit account and payment account information—crucial foundational data that most financial service providers use to assess creditworthiness and offer new services that better meet customer needs.

- **Consolidated Account Information:** Individuals and businesses can manage their financial accounts through a single, centralized mobile application, viewing their account information from different providers and easily sharing it to other service providers.
- **Enhanced Data Accessibility:** Service providers can access and utilize customer data from multiple sources, such as transaction history with various financial institutions. This facilitates data processing, reducing service delivery costs and steps.
- **Innovative Services:** New services have emerged based on the utilization of aggregated data. For instance, in the UK and South Korea, there are services that collect customer data to calculate preliminary credit scores and share this information with multiple lenders, subject to customer consent. In Singapore, aggregated data is analyzed to offer personalized savings, investment, and life insurance services.

In the case of Thailand, the Bank of Thailand (BOT) expects that when customer data can flow smoothly and service providers can use this data to get to know and understand customers better, service providers will be able to design and offer financial services that are more suitable and tailored to each customer's needs. For example, if a customer needs

funds, they can offer loans with appropriate credit limits, interest rates, and repayment periods based on the customer's ability and income and expenses. If the customer has money left over, they can advise the customer to invest the money to find better returns with acceptable and suitable risks for that specific customer.

To facilitate secure and convenient data sharing between service providers and agencies, many countries have enacted laws or regulations by the government or central bank. Additionally, they have involved relevant stakeholders in designing and developing common standards and guidelines for data portability and sharing through these mechanisms, ensuring uniformity, security, and reduced costs and redundancy in standard development.

For Thailand, the BOT, along with other government agencies, financial regulators, and relevant financial service providers[2] is driving the Your Data initiative. This aims to create a digital mechanism that is convenient, secure, without undue restriction and practical to empower customer rights on their data stored at both financial and non-financial sector entities. Such data are later utilized to provide customers with better access and financial services, particularly appropriate access to formal credit and personalized financial management. The initial data sets that will be facilitated through this mechanism include:

1. **Data from financial sector entities:** This encompasses income, expenses, spending patterns, debt repayment behavior, and financial asset holdings. The data will be sourced from service providers under the BOT's supervision, including deposit account information, payment account information (e-money and credit cards), and credit account information. The BOT will mandate providers under its supervision to establish data and mechanisms that allow customers to conveniently, securely, without undue restriction and practically share this information. For data related to securities holdings and insurance policies, the BOT will collaborate with the Securities and Exchange Commission (SEC) and the Office of Insurance Commission (OIC) to develop a mechanism enabling customers to share data among those financial service providers.

[2] Ministry of Finance, Securities and Exchange Commission, Office of Insurance Commission, Revenue Department, Digital Government Development Agency (DGA), Metropolitan Electricity Authority (MEA), Provincial Electricity Authority (PEA), Metropolitan Waterworks Authority (MWA), Provincial Waterworks Authority (PWA), and related financial service associations such as the Thai Bankers Association, Government Financial Institutions Association, Association of International Bank, Personal Loan Club, Thai E-Payment Trade Association, Thai Fintech Association, Association of Thai Securities Companies, Association of Investment Management Companies, Thai General Insurance Association, and Thai Life Assurance Association.

2. Data from non-financial sector entities: This includes income, expenses, and other spending behaviors. The BOT is working with the Digital Government Development Agency (DGA), relevant utilities agencies, and the Revenue Department to develop a channel enabling individuals to share with financial service providers their electricity and water usage and payment data, as well as tax-filing information. It is anticipated that customers will be able to share this data starting in 2025.

To facilitate a mechanism allowing customers to exercise their right to share data held by financial service providers under the BOT's supervision, it is necessary to rely on:

(1) The establishment of rules and regulations, whereby the BOT will issue a regulation requiring BOT-regulated service providers holding customer data to prepare data and establish data sharing mechanisms in a format that allows customers to conveniently, securely, and without undue restriction exercise their rights; and

(2) The involvement of relevant stakeholders, whereby the BOT will collaborate with relevant service providers, and agencies to develop common standards and guidelines for data sharing[3] to ensure practical implementation. This will be carried out through a steering committee and working groups[4] comprising representatives from various types of service providers and relevant associations that will participate as both data providers and data consumers, including commercial banks, specialized financial institutions (SFIs), credit providers, payment service providers, financial technology (fintech) providers, standards development agencies, and relevant regulatory agencies. Consumer and SME representatives will also serve as advisory members.

This document aims to gather feedback on the regulatory framework for service providers to establish mechanisms that allow customers to exercise their right to share their data held by financial service providers (draft regulation). The goal is to enhance financial services to better meet customer needs, particularly in terms of appropriate access to credit and personalized financial management. Initially, the focus will be on enabling data

[3] This will encompass standards for data sharing and security (data & IT security), Application Programming Interface (API) standards, related practices and processes such as data collection and sharing in accordance with data governance and privacy principles, the design of user-friendly interfaces and the creation of a positive customer experience and troubleshooting and problem resolution.

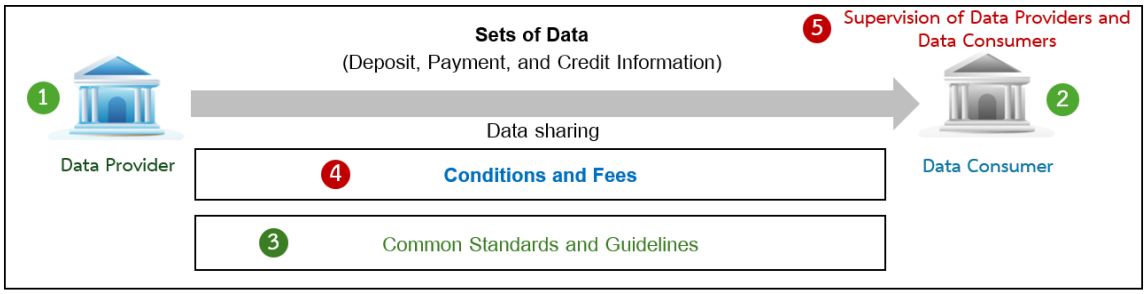
[4] The steering committee and working group consist of representatives from the BOT, Thai Bankers Association, Government Financial Institutions Association, Association of International Bank, Personal Loan Club, Thai E-Payment Trade Association, Thai Fintech Association, the Electronic Transactions Development Agency, and experts. Additionally, there are regulatory agencies that will provide advice and connect policies that may extend to other sectors. Representatives from consumers and SMEs will also provide input on service models that meet their needs.

consumer service providers to utilize customer data to improve and offer better financial services. In the next phase, the BOT will consider the regulatory framework for Third-Party Data Aggregators, who, with customer consent, collect and manage customer data from various sources. These aggregators will display and allow customers to manage their data in one place, assist with preliminary analysis or processing, such as initial credit scoring, and facilitate the sharing of customer data to other service providers or agencies.

2. KEY PRINCIPLES

Individuals as data owners have the right to request that the data collector shares their data to other entities through automated means. This is applicable if the data collector has prepared the data in a machine-readable format and has an automated data sharing system in place to support the data owner's rights under Section 31 of the PDPA.

Therefore, the BOT requires service providers under its supervision to establish such mechanisms that allow data-owning customers to exercise their right to share their data held by the service provider conveniently, securely, and without undue restriction, as follows.



Desired Outcomes (Green Line)

1) Data Providers: Financial service providers holding significant amount of customer data must establish data and mechanisms that allow customers to conveniently exercise their right to share data through digital channels (GL1).

2) Data Consumers: Service providers must be able to utilize the customer data received to develop and offer financial services that meet specific customer needs, especially for appropriate access to formal credit and personalized financial management. This includes third-party data aggregators, for which the BOT will consider additional regulations in the future (GL2).

3) Data Sharing Mechanism: Data exchange between data providers and data consumers must adhere to established common standards and guidelines to ensure efficiency and avoid unnecessary burdens or costs (GL3).

Undesired Outcomes (Red Line)

1) Conditions and Fees: Conditions and fees are obstacles to service usage or data sharing (RL1.1). There are excessive data requests or one-sided data sharing without reciprocal sharing (RL1.2).

2) Inadequate Risk Management: Appropriate oversight is essential, particularly regarding data security, data privacy, and consumer protection (RL2).

3. KEY DETAILS OF THE REGULATION ENABLING CUSTOMERS TO EXERCISE THEIR RIGHT TO SHARE THEIR DATA HELD BY FINANCIAL SERVICE PROVIDERS[5]

3.1 Scope of Financial Service Providers Required to Have a Mechanism that Enable Customers to Exercise Their Right to Share Their Data upon Customer Request (Data Provider)

Principle: *The requirement for service providers to establish mechanisms that enable customers to conveniently exercise their right to share data through digital channels must:*
(1) Cover financial service providers that collect significant amount of customer data to ensure that the data can be effectively utilized, particularly for appropriate access to formal credit and personalized financial management (GL1), and
(2) Not impose excessive costs on such service providers (GL3)[6]

The BOT will mandate financial service providers under its supervision that hold significant amount of customer data, such as deposit account information, e-money and credit card transaction data, and loan information,[7] to establish mechanisms allowing customers to conveniently share their data through digital channels when exercising their rights.

1) Financial institutions and specialized financial institutions (SFIs) under the Financial Institutions Business Act that provide significant amount of deposit services to customers, with a minimum of 100,000 deposit accounts[8], must establish data sharing mechanisms[9].

2) Wide-coverage payment service providers with significant transaction volumes, comprising: (1) e-money providers that offer e-money services usable beyond their

[5] The BOT will utilize its authority under the different bodies of laws to regulate various types of service providers, including (1) Financial Institution Business Act B.E. 2551, (2) Revolutionary Council Announcement No. 58 and related notifications and (3) Payment System Act B.E. 2560.

[6] Brazil and the United Kingdom use this factor to determine the scope of service providers that must establish such mechanisms.

[7] Including commercial banks, finance companies, credit foncier companies, specialized financial institutions, regulated personal loan providers, regulated nano finance providers, credit card issuers, e-money providers, and peer-to-peer lending platform providers.

[8] The 100,000-account threshold is calculated based on a 12-month average of the number of deposit accounts, starting from the month before the regulation takes effect and counting back for 12 months. If the average later decreases below the threshold, the service provider must continue to maintain the data sharing mechanism.

[9] According to data from 2023, the defined service providers cover 99.5% of total deposit accounts.

own business operation and affiliates,[10] and (2) credit card issuers; each with an annual transaction volume of at least 1 million[11], must establish data sharing mechanisms[12].

3) All regulated credit providers[13]: all regulated credit providers must establish a mechanism enabling customers to share or utilize their data, as retail customers and SMEs utilize credit services from both large and small providers.

3.1) Credit providers with at least 100,000 loan accounts or outstanding loans of at least 1 billion baht[14] must either: (1) become a member of the Credit Information Company, or (2) establish a data sharing mechanism in accordance with this draft regulation.

3.2) Credit providers with fewer than 100,000 loan accounts and outstanding loans below 1 billion baht may, in addition to the options in 3.1, choose to provide a channel for customers to retrieve their data in a machine-readable format for their own use or share to other providers. The BOT will further discuss with relevant parties to explore ways to reduce the burden of implementing such mechanisms for these smaller providers.

Furthermore, deposit-taking institutions and payment service providers that do not fall within the mandatory scope for establishing the aforementioned mechanisms[15], but wish to receive customer data under these guidelines, may voluntarily opt in according

---

[10] Refer to e-money providers that require a relevant license to operate their businesses in accordance with Section 2 under 2.2 of Notification of the Ministry of Finance Re: Stipulation on Designated Payment Services. Some e-money providers may have licenses that permit them to provide e-money services on a wide scale (Section 2 under 2.2). However, some of their products may have limited scope (as mentioned in 2.2.1 – 2.2.4). For example, an e-money provider might issue e-money for other companies as clients or business partners for use within those companies' businesses. The BOT will allow these e-money providers to request exemptions from reporting transaction data for these limited-scope products on a case-by-case basis.

[11] This refers to all transactions of the service provider, including payments for goods and services, utility payments, top-ups, withdrawals, and transfers. The annual transaction volume must be at least 1 million transactions, calculated from the total transaction volume over 12 months out of the last 14 months, excluding 2 months with the lowest and the highest transactions and counting back from the month before the regulation takes effect.If the sum later decreases below the threshold, the service provider must continue to maintain the data sharing mechanism.

[12] According to data from 2023, the defined service providers cover 99.9% of total transactions.

[13] Refer to lenders, e.g., financial institutions, SFIs, personal loan providers, nano-finance providers, credit card issuers, and peer-to-peer lending platform providers.

[14] The number of accounts subject to this draft regulation is calculated using a 12-month average of the number of loan accounts and the average outstanding loan balance, starting from the month before the regulation takes effect and counting back for 12 months. If the average later decreases below the threshold, the service provider must continue to maintain the data sharing mechanism.

[15] In accordance with 3.1 1) and 2)

to their readiness. They must also act as data providers based on the principle of reciprocity and adhere to the regulation, common standards and guidelines.

3.2 Scope of Service Providers that can Receive Customer Data (Data Consumers)

Principle: *The determination of financial service providers eligible to receive customer data should:*
(1) Cover financial service providers capable of utilizing customer data to develop and offer services that better meet customer needs, particularly for appropriate access to formal credit and personalized financial management outlined above (GL2), and
(2) Enable appropriate oversight to ensure the security of data sharing and adequate customer protection (RL2).

Financial service providers that can receive customer data under these regulations are those capable of utilizing customer data to enhance their service offerings and are subject to appropriate data governance and security standards.[16] This includes:

1) Financial service providers under the BOT's supervision: This includes financial institutions and SFIs under the Financial Institutions Business Act, payment service providers, and credit providers under the BOT's supervision. These entities can utilize the received data to develop and offer financial services that address appropriate access to formal credit and personalized financial management.

2) Other regulated service providers under similar regulatory regime: Initially, the focus will be on financial service providers regulated by the SEC and the OIC. Both the SEC and the OIC are considering regulations and guidelines for data sharing to ensure consistency. In the future, the scope could be expanded to include service providers in other sectors that meet similar regulatory standards.

Data consumers holding customer data should also provide mechanisms for customers to share their data to other providers, acting as both data providers and data consumers (based on the principle of reciprocity).[17]

Regarding third-party data aggregators, given the need for additional oversight to ensure security and compliance, the BOT will develop specific regulations for licensing and

[16] Examples of countries that have adopted this approach include India, Australia, and the United Kingdom.

[17] Working groups are tasked to establish common standards and guidelines for participation and data exchange under this draft regulation. This includes the participation conditions for service providers who have customer data, who should act as both data consumers and providers.

supervising these entities. This will be aligned with the timeline for enabling customers to exercise their data sharing rights within the financial sector, expected to be by 2026.

3.3 Conditions and Fees Principles Related to Data Sharing

Principle: *When determining conditions and fees principles related to data sharing, the following principles should be considered:*
(1) Promoting Customer Usage: conditions and fees should not hinder customers from exercising their rights or discourage service providers from participating in data sharing (GL1 and RL1.1).
(2) Preventing Excessive Data Requests: Fees principles should be structured to prevent excessive data requests (RL1.2).

When setting conditions and fees principles related to data sharing, service providers must adhere to the following principles:[18]

1) Conditions: Service providers must not impose conditions or take actions that hinder data sharing or utilization. This includes making the participation or usage process overly complicated or setting time limits or usage frequency restrictions that are too restrictive and become obstacles.

2) Fees principles: Generally, no fees should be charged for customers exercising their right to share their data under this draft regulation, as this is a customer's right.[19] However, in cases where data requests significantly exceed a predetermined threshold, fees may be charged to the data consumer to discourage excessive requests. If the excessive data requests are initiated by the customer, the customer may be charged a fee.[20] Any fees charged to either the data consumer or the customer must be agreed upon by the Steering Committee and working groups, in compliance with relevant regulations,[21] reasonable and not hinder the customer's exercise of their rights. Moreover, these fees must be disclosed to the customer in accordance with BOT regulations.

[18] The BOT will collaborate with service providers and relevant stakeholders in the project's steering committee and working group to further specify conditions and fees related to data sharing, including a level of predetermined threshold.

[19] This is aligned with the approaches of many countries, such as the United Kingdom and Australia.

[20] For example, countries like Brazil have implemented measures to prevent customers from requesting excessive data. For instance, financial institutions in Brazil can set limits on the number of transactions per minute or per second that a customer can request. Similarly, in the United Arab Emirates, service providers can charge customers fees for excessive data requests.

[21] E.g., BOT Notification re: Regulations on Market Conduct

3.4 Oversight of Consumer Protection and Data Sharing to Ensure Compliance with Industry Standards and Security

Principle: *The oversight framework for consumer protection and data sharing to ensure compliance with industry standards and security should:*
(1) Ensure adequate consumer protection and risk management (RL2); and
(2) Avoid imposing excessive burdens or costs on service providers, and not hinder data sharing (RL1 and GL3).

The oversight framework will cover consumer protection, personal data privacy, and data sharing to ensure compliance with industry standards and data security. Aligning with international practices,[22] this is to provide customers with confidence in exercising their right to share data throughout the process, as follows:

1) Consumer Protection and Data Privacy: Service providers involved in data portability or reception must:

1.1) Comply with relevant laws regarding consumer protection and data privacy, such as the PDPA and the BOT's regulations on market conduct.

Examples of Laws and Guidelines Related to Consumer Protection and Data Privacy:

(1) PDPA establishes principles for handling personal data when data controllers collect, use, or disclose personal data based on consent. For instance, service providers must obtain consent from the data subject before or at the time of collecting, using, or disclosing personal data. This consent must be explicit, with the purpose clearly stated and separated from other information. The consent form or statement must be easily accessible and understandable, not misleading or deceptive. Additionally, the withdrawal of consent must be made as easy as giving consent.

(2) BOT's Regulations on market conduct, payment systems and supervision of non-bank businesses.[23] The BOT has established regulations for handling consumer data that service providers must follow. For example, when disclosing customer data to third

[22] In line with international regulatory practices, such as those in Brazil, the United Arab Emirates, and Australia, regulations will be established for data sharing, covering the stages before, during, and after a customer exercises their rights. This includes procedures related to obtaining consent, verifying identity, and confirming the data sharing request. Data sharing must adhere to specified standards, and consumers must be able to easily manage their data rights. Adequate information security measures must be in place, and there should be a clear process for addressing complaints.
[23] Please refer to relevant BOT Notifications that addresses market conducts on financial institutions, SFIs, lenders, payment service providers and Peer-to-peer lending platforms.

parties, there must be processes to ensure that the recipient can securely protect the data. Service providers must collect only necessary data and use it for the purposes specified by the customer. They must keep customer data confidential, disclosing it only as required by law or with the customer's consent. There must also be convenient channels for customers to withdraw their consent.

(3) Regulations under the Anti-Money Laundering Law[24]: Service providers are required to identify and verify the identity of customers in accordance with the risk associated with the product or service. The BOT has established additional regulations for transactions involving the opening of deposit accounts and e-money.[25]

1.2) Comply with additional guidelines set by the BOT regarding data privacy throughout the data sharing process. This is to prevent unauthorized data requests or usage without the customer's consent, or by those who are not the actual customers, as follows:

1.2.1) Obtaining Consent from Customers: To enable data providers to share data to data consumers, the following minimum requirements must be met:

(1) Separate the consent request for data sharing under this draft regulation from other consent requests and clearly distinguish it from other matters.

(2) Provide sufficient information and conditions to the customer for them to make an informed decision about exercising their data portability rights.[26] This must include at least:

(2.1) The types and items of data for which consent is being requested.

(2.2) The purpose of data usage, which must be for the service or transaction for which the customer has given consent and must fall within the business scope defined by relevant regulatory laws or authorized by the respective regulatory authority.

(2.3) The duration of the consent, which must align with the purpose of data usage. Consent may be requested for a single data request or for a specified

[24] Please refer to: https://sed.amlo.go.th/uploads/content_attachfile/attach_202005150837_5ebdf25851ee2.pdf and https://ses1.amlo.go.th/content/index/53

[25] See e.g., https://www.bot.or.th/content/dam/bot/fipcs/documents/FPG/2562/EngPDF/25620191.pdf

[26] Aligned with those in Brazil, Australia and UAE.

period.[27] If consent is requested for a period, it must not exceed 12 months[28] to allow the customer to review the necessity and appropriateness of the consent.

(2.4) The names of the service providers who will use the data to provide services to the customer.

(2.5) The names of individuals or entities involved in managing the customer's data on behalf of the data consumer, such as third parties contracted by the service provider to collect and/or process the customer's data, or to facilitate connecting the data sharing system as per the customer's consent.

1.2.2) Data providers must implement processes for customer authentication and authorization before sharing data to data consumers as per section 1.2.1, after receiving a request along with consent. This ensures that the customer is the rightful user and genuinely intends to exercise their rights.

(1) Customers must perform authentication at Authenticator Assurance Level (AAL2)[29] or use two-factor authentication (e.g., PIN and OTP).[30] This level aims to strike a balance between accessibility and security: not too high to hinder customers' exercise of their rights, nor too low to risk unauthorized transactions.

(2) Customers must perform authorization before data sharing by:

(2.1) Separating the authorization request under this draft regulation from other requests and clearly distinguishing it from other matters.

(2.2) Providing sufficient information and conditions for the customer to make an informed decision about granting authorization, similar to the consent process in section 1.2.1 (2.1) and (2.2). The authorization period must align with the purpose and duration of the consent. The names of the data providers who will share the data and the names of individuals or entities involved in managing the customer's data on behalf of the data provider must also be disclosed.

---

[27] Period-based consent is often seen in financial products that help manage finances according to individual customer behavior. For example, a customer may give recurring consent for 12 months to allow their account information from multiple service providers to be displayed in a single mobile application for the entire 12-month period. This helps in planning income and expenses, savings, and investments.

[28] Aligned with those in Brazil, Australia and UAE.

[29] Aligned with those in UK and Australia

[30] 2-Factor Authentication is used for money transfers and payment of amounts less than 50,000 baht.

1.2.3) Data providers and data consumers must ensure that customers can easily manage and verify their consent and authorization, and inform relevant parties of these actions as follows:

(1) Service providers must provide evidence of the granting, amending, and withdrawal of consent and authorization to the customer through the channels specified by the customer, such as email, application, or the service provider's service channels, to allow the customer to verify their consents.

(2) Service providers must provide channels for customers to easily manage their consent and authorization, accommodating changes, withdrawal, and review of consent and authorization history.

(3) Data providers and data consumers must inform the customer and the other service provider when consent or authorization is changed, withdrawn, or expired, as applicable, to prevent data requests, usage, or sharing without the customer's consent. When the consent or authorization is still valid, the service provider must remind the customer of the existence of such consent and authorization at least every 90 days.[31]

The BOT will further establish guidelines on consent and authorization in collaboration with relevant stakeholders through the Steering Committee and working groups.

2) Data Portability in Compliance with Common Standards and Secure Data Management:

2.1) Data providers and data consumers must comply with the common standards and guidelines set by the BOT. This includes formats and processes related to consent, authentication, and authorization, user-friendly design for a positive customer experience, data connection, storage, and sharing methods, as well as problem resolution. BOT will collaborate with relevant stakeholders through the Steering Committee and working groups of the Your Data project to develop and enforce these common standards and guidelines.

[31] Aligned with those in Australia (Regulations on Consumer Data Right) and UK (Customer Experience Guideline)

2.2) Data providers and data consumers must implement effective data management practices to ensure customer data security. This includes governance, information technology security, and incident or problem management, as follows:

2.2.1) Data Governance: Service providers must implement data governance practices to ensure that all data transferred and related processes are managed securely and with respect for data privacy, as follows:

(1) The Board of Directors of the Service Provider must prioritize the rights of customers to their data, ensuring data security and privacy, and must oversee the strict and continuous implementation of these matters by:

(1.1) Establishing and approving policies that emphasize the rights of customers to share their data, ensuring data security and privacy. These policies must cover the entire data lifecycle management and be reviewed at appropriate intervals or when significant changes occur.

(1.2) Responsible for taking overall supervision and overseeing that the organizational structure can support the practical implementation of customer data sharing rights. This includes appropriate review and balance of operations, considering the size, nature of business operations, business complexity, and data risk of the service provider.

(1.3) Overseeing that senior management (i) communicate the policy to relevant personnel within the organization, emphasizing its importance and ensuring they understand their roles and responsibilities and (ii) drive relevant personnel to strictly and continuously implement the established policies.

(1.4) Overseeing the allocation of resources to support the implementation of customer data sharing rights and data security and privacy to achieve the desired outcomes.

(1.5) Monitoring and overseeing the overall implementation of customer data sharing rights, data security and privacy, ensuring compliance with relevant guidelines and policies. This includes ensuring that management: (i) regularly report operational progress and risks to senior management and at least annually to the board of directors, for the purpose of reviewing relevant policies and strategic plans. (ii) promptly

report significant risks and issues that may materially impact service provision, operational status, or the service provider's reputation to the board, for the purpose of directing preventive or corrective actions in a timely manner.

To enhance the efficiency and effectiveness in operations, the board of directors may delegate the following tasks to subcommittees or designated individuals: (a) review policies on behalf of the board, provided that the board is informed of the review, and if there are significant changes, they must be submitted to the board for approval, (b) oversee the detailed organizational structure and role assignments within the overall organizational structure previously approved by the board, and (c) monitor operational reports and significant risk issues from management, provided that an overall summary of operations is reported to the board at least annually, and significant risk issues are promptly reported to the board.

In cases where delegation occurs, the board of directors must clearly define the roles, responsibilities, and authority of the subcommittees or designated individuals. The board must also regularly monitor the overall operations and significant risk issues reported by the subcommittees or designated individuals. This oversight ensures that the service provider can appropriately and timely address any issues that arise, as well as identify and implement improvements to prevent recurrence of such problems in the future.

(2) Senior Management of the Service Provider must drive and ensure the strict and continuous implementation of policies approved by the board of directors, by:

(2.1) Communicating and driving the implementation of the approved policies to relevant personnel within the organization in a concrete and rigorous manner.

(2.2) Establishing a clear organizational structure, defining detailed responsibilities and roles within the overall organizational structure previously approved by the board, and ensuring sufficient resource allocation to support the implementation of customer data sharing rights, data security, and privacy to the desired outcomes.

(2.3) Monitoring the implementation of customer data sharing rights, data security and privacy, ensuring compliance with relevant regulatory guidelines and policies set by the board. This includes reporting these matters at least annually to the board, subcommittees, or designated individuals, and promptly reporting significant risks and issues that may materially impact service provision, operational status, or the service provider's reputation to the board.

However, Service providers that are branches of foreign commercial banks or foreign financial service providers in Thailand must comply only with the senior management responsibilities outlined in section 2.2.1 (2).

2.2.2) Information Technology (IT) Security: Service providers must implement secure IT management to appropriately protect customer data and effectively prevent and respond to cyber threats and data breaches. This must be done in accordance with the minimum IT security standards set by the BOT (annex).[32] Details include:

- Proper IT asset management.
- Data security throughout the data lifecycle.
- Access control to prevent unauthorized access to systems and customer data.
- Security of communication networks, servers, and operational equipment.
- Establishment of IT security standards.
- System monitoring and threat surveillance.
- Secure system procurement, and development according to international standards.
- Third-party risk management.

[32] Commercial banks, SFIs, and significant payment service providers are already required to comply with these minimum standards. Non-significant payment service providers and non-bank businesses must additionally comply to meet these standards. The qualifications of significant payment service providers are specified in section 3.2 (3) of the BOT Notification No. SorNorChor. 1/2564 on Information Technology Risk Management under the Payment Systems Act.

- Maintaining audit trails and logging data sharing activities to trace access and usage of customer data, which is beneficial for legal proceedings and identifying offenders and/or responsible parties in case of data breaches or leaks.[33]

2.2.3) Incident and Problem Management: Service providers must implement appropriate and timely incident and problem management for issues arising from customer data portability rights, such as data breaches and cyberattacks in both IT systems and other operational risk management aspects,[34] as follows:

(1) Implement robust processes for incident and problem response aligned with risk levels, to ensure appropriate and timely handling and resolution. This includes prompt problem resolution, investigation, root cause analysis, impact assessment, and developing plans to prevent recurrence.

(2) Report incidents or problems to senior management and/or relevant committees based on risk levels. For severe incidents or those that may significantly impact service provision, operational status, or the service provider's reputation, the board must be informed promptly.

(3) Resolve issues and handle complaints in compliance with existing BOT regulations on problem resolution and complaint management.[35] This includes key aspects such as appointing personnel to handle complaints, providing complaint channels to customers, establishing standardized processes for handling issues and complaints, ensuring fair resolution, regular monitoring, customer redress measures, and preventing recurrence of issues or complaints.[36]

However, if service providers intend to share customer data under these regulations through alternative mechanisms, they must consult with the BOT beforehand to ensure that

---

[33] The BOT will, in collaboration with other stakeholders, create guidelines for liability distributions in due course.

[34] See BOT Notifications regarding IT risks for financial institutions, SFIs and payment service providers.

[35] Refer to relevant BOT Notifications that addresses market conducts on financial institutions, SFIs, lenders, payment service providers and Peer-to-peer lending platforms.

[36] Commercial banks, SFIs, credit card providers, personal loan providers, and nano finance providers must already comply with Notifications regarding market conduct. However, currently, payment service providers and peer-to-peer lending platform providers have less stringent requirements for complaint management compared to other service providers. Therefore, it will be required that these service providers, who will exchange data under this draft regulation, must comply with the complaint resolution and management requirements equivalent to the Market Conduct Regulation. This applies to non-bank entities with total outstanding loans below the significant level specified by the BOT (as per Attachment 11 of the Market Conduct Regulation on complaint resolution).
If, in the future, specific requirements for payment service providers and peer-to-peer lending platform providers are imposed, they should be followed.

such data transmission through these mechanisms complies with the requirements of these regulations.

3.5 Supervision Process to Ensure Service Providers' Compliance with Standards:

The BOT will continuously supervise data providers and data consumers to ensure compliance with these guidelines, maintaining standards from before the commencement of customer data sharing services, during service provision, and in the event of problems or disputes with customers. This supervision aims to ensure the security and standardization of data sharing and management comply with established regulations, common standards and guidelines as follows:

1) Before the commencement of customer data sharing services:

1.1) Service providers must pass tests for compliance with common standards and guidelines and be assessed by BOT for readiness and qualifications according to BOT's criteria. Service providers qualified as data providers and data consumers under these guidelines must:

1.1.1) Submit documents demonstrating readiness and qualifications according to the common standards and guidelines to the BOT.[37]

1.1.2) Undergo testing for compliance with the standards and guidelines set by the BOT with the data sharing service provider registry system (Directory).[38] If the service provider passes BOT's assessment as per 1.1.1) and the tests for compliance, they will be registered as a member of the Directory.

1.2) The BOT will publish the list of service providers registered in the Directory, including the start date of services, on the BOT's website for service providers and customers to access.

2) During the provision of data sharing services:

2.1) Service providers must submit data and/or reports related to the services under this draft regulation as specified by the BOT or upon the BOT's request.

---

[37] In the case where data consumers under this draft regulation are service providers regulated by other agencies, those regulatory agencies are responsible for assessing the readiness and qualifications of the entities under their supervision and informing the Directory for consideration of registration. The BOT will consult with these regulatory agencies to ensure that the assessment of readiness, qualifications, and compliance with various criteria are standardized.

[38] The BOT is in consideration on selection of the Directory's service provider.

This is to monitor usage development, obstacles, and service supervision, such as the number of consents received from customers categorized by data usage purpose, the number of data requests (e.g., API calls), the success and failure rates of data requests, service issues, and complaints.

2.2) BOT will continuously monitor and supervise service providers. If any issues or deficiencies in the system or services are found under this draft regulation, the BOT may order the service provider to rectify them within a specified period. If a service provider fails to improve or rectify issues or deficiencies that may significantly impact the system or data sharing services under these guidelines, or if the service provider's status or operations pose a risk to public interest, the BOT may order the suspension of all or part of the data sharing services, including prohibiting new business related to such data sharing services. Additionally, the BOT may impose fines in accordance with relevant laws or may notify the Directory to consider revoking registration of the service provider from the Directory.

3) In the event of problems or disputes with customers[39]

3.1) Service providers must promptly report significant issues or incidents to the BOT[40] upon occurrence or awareness, including causes and corrective and preventive measures to avoid recurrence. This must be done after analysis and development of such measures, and must cover at least the following issues or incidents:

(1) Issues or incidents that may significantly impact the system or data sharing services under these guidelines, or that may pose a risk to public interest.

(2) Issues or incidents that internal policies require reporting to the highest-ranking executive and/or relevant committees.

(3) Incidents where the service provider's IT systems are attacked or threatened.

3.2) Service providers responsible for the issues or incidents must appropriately address, rectify, and compensate customers according to laws, regulations, and guidelines.[41]

---

[39] See also the penalty section of the PDPA.

[40] Significance is determined based on the level of risk and impact, such as the number of affected customers, the volume of affected data, and the potential damage, both in terms of financial loss and reputational harm to the involved parties.

[41] The BOT will, in collaboration with other stakeholders, create guidelines for liability distributions in due course.

3.6 Implementation Schedule

The BOT has determined that service providers must complete the necessary mechanisms and be ready to allow customers to exercise their right to share information to other service providers as per their readiness, by (1) starting with deposit information, followed by credit and payment information, as it can be developed based on the existing deposit information standards from the dStatement service,[42] (2) starting with individual customer information, followed by juristic customer information, to allow service providers time to develop systems for verifying and authenticating juristic identities and to support the different user journeys for juristic information which differ from those for individual information.

Estimated timelines are as follows:

1. Individual deposit information: Service to be available within 6 quarters from the effective date of the guidelines (expected by Q4 2026).

2. Individual credit and payment information: Service to be available within 7 quarters from the effective date of the guidelines (expected by Q1 2027).

3. Juristic deposit information: Service to be available within 9 quarters from the effective date of the guidelines (expected by Q3 2027).

4. Juristic credit and payment information: Service to be available within 10 quarters from the effective date of the guidelines (expected by Q4 2027).

After this draft regulation come into effect, service providers who, as of the effective date, do not yet meet the criteria for implementing mechanisms, must monitor the number of accounts, outstanding balances, or transaction volumes on a fiscal year basis. If they meet the criteria specified in section 3.1, they must complete and make available the customer data portability mechanisms within 4 quarters from the end of the fiscal year in which the service provider meets the criteria specified in section 3.1 for individual data. An additional 3 quarters are provided for juristic data.

However, in cases of necessity due to factors beyond the service provider's control, the service provider may request an extension or an exemption from the BOT on a case-by-

[42] Refer to: https://www.bot.or.th/en/financial-innovation/digital-finance/open-data/digital-bank-statement.html

case basis, providing reasons, necessities, and relevant details. The BOT may grant or deny the request or impose additional conditions as deemed appropriate.

4. IMPLEMENTATION TIMELINE OF YOUR DATA PROJECT

4.1 Implementation timeline in the financial sector

Period	Implementation progress in the financial sector (Coordinated with the capital market and insurance sectors)
Present – March 14 2025	BOT will seek public feedback on the draft regulation on the oversight of mechanisms enabling customers to exercise their right to share their data held by financial service providers
Within Q2 2025	BOT will issue the regulation on the oversight of mechanisms enabling customers to exercise their right to share their data held by financial service providers, which will come into effect.
Within Q3 2025	BOT will announce the common standards and guidelines for the first set of data, developed in collaboration with service providers and relevant agencies.
Within Q4 2026	Service providers will begin offering the first set of data sharing services (individual deposit account information).
Within 2026	BOT will issue a regulation for the authorization and supervision of Third-Party Data Aggregators.

4.2 Implementation progress in the non-financial sector

The BOT is actively collaborating with the Revenue Department, the DGA, the Metropolitan Electricity Authority, the Provincial Electricity Authority, the Metropolitan Waterworks Authority, and the Provincial Waterworks Authority. The objective is to develop mechanisms that enable citizens to share their tax information, as well as electricity and water usage and payment data, to financial service providers. This service is expected to be available to customers by 2025.

5. EXPECTED OUTCOMES

The BOT, in collaboration with relevant agencies, aims to develop mechanisms enabling customers to exercise their right to share their data conveniently, securely, without undue restriction, and practically. The goal is to enable individuals and businesses to use their data from various sources to receive financial services that better meet their needs, particularly: (1) appropriate access to credit, especially for individuals without regular income and small businesses with potential but insufficient financial history with financial institutions. These entities often have other relevant data available elsewhere, and (2) personalized financial management for individual customers and small businesses, addressing a significant gap in the Thai financial system.

The BOT expects that once customers can exercise their right to share their important data from various sources, it will result in benefits for individuals, businesses, and the overall financial system. For example, small businesses and individuals will have better access to credit with appropriate sizes, terms and conditions and receive services that help them manage their finances in a way that suits their lifestyle and career. Additionally, there will be an increase in emergency savings or retirement savings among the population.

The success and practical implementation of these mechanisms require collaborative efforts from all relevant sectors. This includes participation in developing common standards and guidelines and providing feedback on related regulations. The BOT hopes to receive your feedback and suggestions on the draft regulation, which will be incorporated into the development of the regulations. Initially, it is expected that the regulations will be issued by Q2 2025.

Feedback and suggestions on the draft regulation can be submitted to BOT through the following channels until March 14, 2025:

(1) Download the feedback form from the BOT website (www.bot.or.th) and send it to the Financial Institution Strategy Department, Financial Institution Policy Group, BOT via email: opendata-fsd@bot.or.th

(2) Provide feedback through the Central Legal System website (law.go.th)

ANNEX

Minimum Requirements for Data Security in Information Technology for service providers involved in receiving or sharing data under this draft regulation.

1. **IT Asset Management:** Service providers must maintain a comprehensive inventory of IT assets related to their services. This inventory should be used to establish appropriate control measures based on the risk level of each asset.

2. **Information Security:** Service providers must manage data securely, ensuring that data handling aligns with information classification standards and covers the entire data lifecycle, from creation or collection to storage, usage, and destruction of data.

3. **Access Control:** To prevent unauthorized access to systems and customer data, service providers must implement multi-factor authentication, especially for high-privilege accounts and user accounts that can access customer data over public networks (Internet).

4. **Communications Security:** Service providers must design and manage secure communication networks in accordance with international standards. This includes protecting against and monitoring for intrusions or threats, particularly at Internet connection points.

5. **Server and Endpoint Security:** Service providers must protect against malware and various attack forms, ensuring that servers and IT endpoints are regularly updated to counter new threats.

6. **Security Baseline and Hardening: Service** providers must configure their systems to meet international security standards. This includes setting a minimum-security baseline and regularly reviewing configurations to ensure compliance.

7. **Data Backup:** Service providers must ensure the availability of customer data in case of primary data failure or damage. Backup data must be managed according to its importance and protected according to its confidential classification level. Regular testing of backup data readiness is also required.

8. **Change Management:** Service providers must implement stringent controls over system changes to ensure security and prevent unauthorized modifications. This

includes key processes such as system deployment, system configuration, and patch installation.

9. Security Patch Management: Service providers must have a robust and timely process for addressing vulnerabilities to reduce the risk of attacks on IT systems. This involves managing security patches according to risk levels and ensuring all systems and devices are covered.

10. Security Monitoring: Service providers must have processes or tools in place to detect, prevent, and respond to abnormal events or cyber threats promptly.

11. Vulnerability Management and Penetration Testing: Service providers must conduct regular vulnerability assessments for critical systems at least annually and perform penetration tests by independent experts, especially for systems connected to public networks (Internet-facing).

12. System Acquisition and Development: Service providers must follow stringent security controls and international standards in system acquisition and development processes:

12.1. System Acquisition: Clear and appropriate criteria must be established for selecting systems and external service providers, considering factors such as system reliability, certification to recognized international standards, system security, support, and maintenance. This ensures that systems and external service providers meet the security standards set by the service provider and align with international standards and can effectively meet operational needs.

12.2. System Development: Service providers must design, develop, and test systems to ensure confidentiality, accuracy, reliability, availability, and security, in accordance with the standards set by the service provider and international standards.

13. Third Party Risk Management: Service providers must have a comprehensive approach to managing risks associated with using services, connecting to, or accessing data from third parties. This includes maintaining security according to risk levels while ensuring the service provider remains responsible for business operations and customer service. The process should cover risk assessment, third-party selection, contract or agreement

formulation, continuous performance monitoring, and termination or conclusion of contracts or agreements.

14. Audit Trail and Logging: Service providers must

14.1. Maintain comprehensive and secure logging of events to trace access and usage of systems or data supporting the services. These logs should also serve as evidence for electronic transactions as required by law.

14.2. Store audit trails for each transaction with at least the following details:

(1) Information on consent and authorization for data sharing.

(2) Information on modifications and revocations of consent and authorization.

(3) Information on data sharing and usage by the data consumer, with a 10-year retention period.[43]

[43] The 10-year retention period aligns with the statute of limitations for data breach claims under the PDPA's civil liability provisions. This aligns with practices in countries like the UK, Australia, and Brazil. Some BOT-supervised service providers already retain data for 10 years for AML compliance.