ASEAN Bankers Association

ASEAN Interoperable Data Framework

Safe and secure cross-border flow of data

Version 1.0 November 2022

Contents

Background and Overview

A. Background and Overview

Data is used to create value and the economic and social values can only be maximised when data can flow freely across borders. Cross-border data flows are the lifeblood of this new economy and will continue to grow. Globally, it is estimated to reach 65% of global GDP by end of 2022[1]. The ability to aggregate, share, store, process, and transmit data both domestically and across borders is critical to the overall financial sector development. Increased data connectivity will intensify cooperation and promote the flow of data within and amongst ASEAN Member States towards a digitally enabled ASEAN network that is secure, sustainable, and transformative; and to enable an innovative, inclusive and integrated ASEAN Community.

Though significant global efforts have been made to harmonise data standards, data governance and data protection frameworks, progress on digital data management issues still vary considerably across ASEAN. The lack of an interoperable data framework results in the ASEAN Member States being at different levels of maturity in terms of data production and open data development, which hence suggests a large potential for further growth. Currently, ASEAN consumers have less access to financial services than their peers in developed markets. Referencing the World Bank, the banking penetration in ASEAN stands at 50% compared to the staggering world benchmark of 95%. This highlights a large portion of the ASEAN community that remains unbanked and underserved.

There is significant opportunity to improve transparency on requirements and identify areas to enhance data collaboration. The expanding use of data in financial services and the increasing use of technology to supply financial services offer a range of benefits, including greater consumer choice, enhanced risk management capabilities, and increased efficiency. The benefits of data connectivity across ASEAN are as follows:

a. **Innovation of new products and services that will benefit especially the underserved and underbanked:**
   Data collected, processed and stored within the institution and flowed on a secured basis can allow a stronger form of meaningful analytics to generate insights on the underbanked and underserved customers, as well as the relevant products and services specially to cater to their needs.
b. **Accessing a more comprehensive suite of information that would influence decision making:**
   Increased data connectivity enables organisations to use common infrastructure to serve multiple markets, so digital goods and services spread to customers more rapidly, which correspondingly increases customer choice and satisfaction.
c. **Improving overall transparency and integrity of the information being shared:**
   Enhanced cross-border data flows provide more scrutiny on the quality of data being shared and more information must be provided by institutions on the data sources, which increases the level of rigour in overseeing and managing data.
d. **Improving efficiency and compliance for AML/CFT programs:**
   Two of the ten ASEAN Member States have instituted a national e-KYC utility in the recent 2 years, demonstrating an increase in demand for a cost-effective and efficient way of checking against sanctions and blacklists. The cost-efficiency can be further improved where such efforts are coordinated regionally across the Member States beyond efforts locally within.

[1] Cross-border data flows: Designing a global architecture for growth and innovation: https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation

Introduction

B. Introduction to the ASEAN Banking Interoperable Data Framework

The objective of the ASEAN Banking Interoperable Data Framework ("IDF" or "Framework") is to create an inter-territory flow of data without imposing such regulatory requirements to override existing policies for interoperability and data regulations that may exist in the ASEAN Member States. The intent of the Framework is to establish minimum practices for safe and secure data sharing. With stronger safeguards and clarity on regulatory compliance, banks across all ASEAN nations will be more ready to interoperate their data and consequently benefit consumers with more personalised goods and services.

As such, in our context, **data interoperability** refers to the ability to access and process data from multiple countries in a safe and secured manner, and which complies with the legal and regulatory requirements of the sharing countries. The data represented must be of agreed quality and baselined against industry best practices and open technical standards, where applicable.

Vision and objectives

The Vision statement was established as "*to facilitate cross-border flow of data in a safe and secure manner for the banking financial institutions within ASEAN Member States.*"

Key Objectives of the ASEAN Banking Interoperable Data Framework

Three key objectives were defined:

1. Foster innovation in financial services - It aims to improve the financial inclusion through greater exchanges of information through trusted data flows which drive transparency in credit worthiness and risks and promote increased trust. With the innovation fostered, it increases customised services and processes to cater for different market segments.

2. Establish interoperable standards for data sharing – The standards help to Improve integrity of information shared with agreed standards of data quality and metadata. Such data standards increase consistency for data collection and data processing and drive greater accountability and transparency on use of data.

3. Foster collaboration and trust - This encourages a culture of collaboration to drive efficiencies and effectiveness through data sharing, such as in financial crime and fraud detection etc. and to build trust in the digital economy and digital banking.

Guiding Design Principles

The design guiding principles were researched and aligned to multiple international cross-border data sharing frameworks and the ASEAN Data Management Framework. The development of the Framework will be underpinned by the following design guiding principles:

1. **Trustworthiness** – It aims to create a trust environment in the data sharing ecosystem and across the data lifecycle, by ensuring best practices around data security, data quality and integrity are adhered to. This would require parties to an interoperable data agreement to put in security controls to prevent unauthorised access or theft by malevolent forces, and handle data in compliance with local regulations and used in accordance to the prescribed purposes. To ensure that data can be trusted, data integrity and quality must be ensured throughout the lifecycle.

2. **Practicality –** The developed Framework and related guidance / standards should be technology-agnostic, be economically viable for implementation and easy to do so.

3. **Standardisation –** Data quality and metadata standards are baselined for collaborative and consistent applications. Where relevant industry best practices and open technical standards are available, these are encouraged. To the extent possible and required, individual ASEAN Member States have the discretion to supplement the Framework with complementary local standards.

4. **Openness** –Data should be legally and technically open to authorised parties for the prescribed purposes of use and the use of such data, enabled by cross-border flows, is encouraged.

Scope of application

1. The IDF is designed to provide voluntary and non-binding guidance based on best practices in the area of data interoperability for banks within ASEAN Member States. The content should not be read as nor constitute as legal advice, nor construed as a tool for compliance to any law and regulations.
2. The IDF is intended to be adapted to varying needs for adoption and tailoring by the member banks to their own systems of managing data.
3. "Data" as used in this IDF refers to all structured data a bank creates, collects, accesses and processes through a system or electronic means. This may include personal data and business transactional data.
4. The IDF is intended for the use of all banks operating in any ASEAN Member State, including branches of banks headquartered outside of ASEAN.

The ASEAN Banking Interoperable Data Framework

C. The ASEAN Banking Interoperable Data Framework

The IDF is adapted from the ASEAN Data Management Framework and comprises the 6 key pillars, namely Governance and Oversight, Policies & Procedural Documents, Data inventory, Impact / Risk assessment, Controls and Monitoring & Continuous Improvement.

These pillars have been adapted to include additional components to facilitate the access to cross-border data and incidental regulatory and legal requirements to be conformed to.

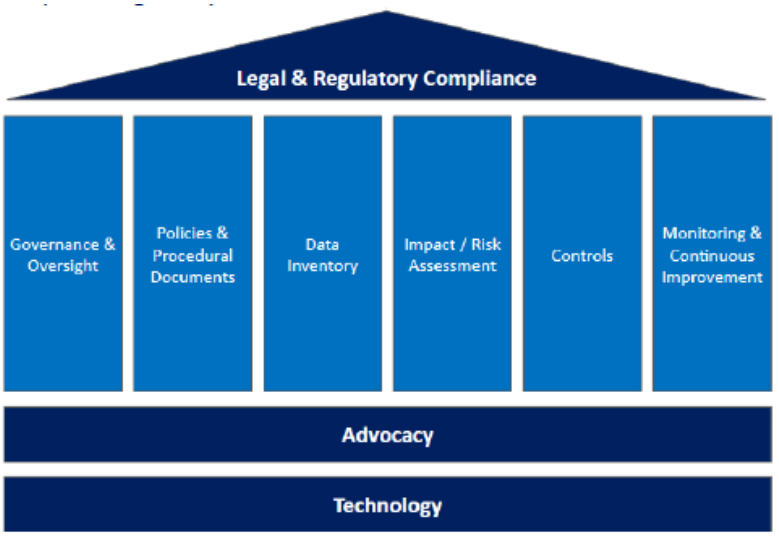

Figure 1: The ASEAN Banking Interoperable Data Framework

The additional domains added to the Framework are termed as the Enablers to data sharing - and are namely, Legal and Regulatory, Advocacy and Technology.

The principles to be considered under each component have been laid out in the sections that follow.

1. LEGAL AND REGULATORY COMPLIANCE

Legal and regulatory compliance standards vary across countries within ASEAN. Depending on the nature of the data to be shared, specific international regulations may also apply. For data interoperability to succeed, it is important to ensure compliance with the requirements set forth in the countries of both the data importer and data exporter and that such compliance to the requirements are understood clearly by both parties.

Legal boundaries

- Boundaries on the sharing of data should be understood and clearly defined, including the right to use the data, prerequisites to the sharing of the data, and limitation on the use of the data in both the exporting and receiving countries.
- Existing policies, standards and published guidance documents to govern the data, enforce data quality and protect the data shall be observed so that minimum standards of data integrity and quality are ensured throughout the data lifecycle.

Permissible cross border data conditions

- Data sovereignty rules may apply to some ASEAN Member States, which restricts the flow of data across borders. Exceptions to allow access to specific types of data may be permitted subject to the meeting of the criteria set forth by the respective departments in the bank. Further details of this may be found in Appendix 1.
- Data sharing agreements shall adhere to the conditions for cross-border data transfer of the data exporting bank. This includes observance of required processes, timeline for approvals and proof of fulfilment of conditions. Such conditions vary from country to country and may include but are not limited to use case justification, cost benefit analysis, parties to the sharing agreement and security measures undertaken.

Personal data protection requirements

- Where the shared data involves personal data, care must be taken to observe the domestic personal data protection legislations, policies or guidelines in both data exporter and data importer countries.
- Where data subjects and the use of the data are beyond the ASEAN Member States, additional international data privacy requirements may apply, e.g. General Data Protection Regulation (GDPR).
- The boundaries and conditions (e.g. consent, time boundaries and specific use case limitations) for use and transfer of personal data across borders shall be observed. Technology and/or process controls should be implemented for rectification/ revocation of consent.
- Clear escalation protocols shall be in place in the event of breaches and measures for the remediation of such breaches should be clearly articulated and understood.

To foster trust through data sharing, formal mechanisms to facilitate such cross-border data transfers must be in place to articulate the scope, legal obligations, roles and responsibilities, escalation protocols and remediations. This is achieved through a cross-border data sharing agreement. Additionally, the APEC Cross-Border Privacy Rules (CBPR) system is another mechanism for banks to safeguard the flow of data while protecting the privacy rights of individuals.

Cross-border data sharing agreement

- A cross-border data sharing agreement shall be developed in accordance with the principles set forth in the ***ASEAN Framework on Personal Data Protection (2016)[2],*** with reference to the

[2] https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

ASEAN Data Management Framework , for internal organization use in conjunction with the ***ASEAN Model Contractual Clauses for Cross Border Data Flows*** where applicable.

- The agreement shall define the parameters for specific relationships between banks, set protocols and procedures for data sharing within the parameters of the law within the exporting and importing countries. This may include, but not be limited to, mutually acceptable security requirements for the infrastructure and the data storage, and the nature, frequency and standards of data that will be shared as part of the agreement.
- Where there are differences between laws/regulations across the countries, the agreement can bridge the gaps between the countries for specific use cases. Limitation on the use of the data can also be included.
- To protect the integrity of the data across its lifecycle and ensure the limitation on the use of the data is in accordance with the agreement, the agreement shall contain a clause for the data importer to perform an audit/inspection certifying the required controls over the use limitation and protection of the data integrity are in accordance with the Service Level Agreement (SLA).
- The data sharing agreement shall include confidentiality clauses, security safeguards indemnification clauses, warranties, penalties, termination, remedies, recourse and arbitration alternatives, where applicable.

APEC Cross-Border Privacy Rules (CBPR) Certification

- The APEC Cross-Border Privacy Rules (CBPR) System is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognized data privacy protections. It is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies.
- Certification is available to banks in our ASEAN Member States to demonstrate adherence to an enforceable standard of best practices and commitment to data privacy.
- As certified companies demonstrate good faith compliance to the enforcement requirements in APEC, data sharing with certified companies serves to increase trust, improve the speed of formalising the agreements, and reduce barriers for the cross-border flow of data. As such, certification is encouraged amongst the ASEAN Member State banks.

2. GOVERNANCE AND OVERSIGHT

At the very heart of managing data to be available for and suitable for sharing with other counterparties lies governance and oversight of the data governance program.

Governance

- Bank leaders should provide their endorsement to the establishment, implementation, operation, monitoring, review, maintenance and facilitation of data sharing initiatives.
- Clear accountability, responsibilities and liabilities should be established among the data exporter, data importer and any other impacted data intermediaries.
- Key stakeholders should be identified to ensure accountability for the entire lifecycle of data sharing, from consent, access, transmission to usage. Responsible parties will also have to be identified to develop and support the use case, risks identification and mitigation.

Key Stakeholder	Key Responsibility
Data Owner	Accountable for the classification, protection, use and quality of one or more data sets to be shared
Data Steward	Responsible for ensuring the quality and fitness for purpose of the bank's data assets to be shared, including the metadata for those data assets
Data User	Responsible for proper use of the data according to the data sharing agreement and principles set in this framework
Technology Owner	Accountable for the technology(ies)[3] used to facilitate secured data sharing
Technology Steward	Responsible for selection and configuration of the data sharing technology(ies)
General/ Legal Counsel	Responsible for drafting, reviewing, and negotiating contracts and agreements to facilitate data sharing[4]

Table 1: Examples of key stakeholder roles and responsibilities

- An independent assessment body (*can be an internally assigned body*) shall be appointed to attest to the adherence to defined data governance standards, policies and other stipulations within the data sharing agreement. This independent assessment body shall report independently to the Risk Committee on their findings and reports.

Controls and Protocols

- Clear Protocols for risk monitoring and agree on acceptable threshold limits between data exporter and importer should be set up[5]. The definition of a reportable breach based on legislation in the exporting and importing countries and the required reporting and communications protocols[6] should be clearly established, and clear escalation paths for complaints management, reporting,

[3] See "Technology" pillar on the principles to select an appropriate technology
[4] See "Legal and regulatory compliance" pillar
[5] See "Impact/Risk assessment" pillar focusing on management of data sharing risks based on the bank's existing risk management framework
[6] See "Controls" pillar on the controls related to data breach response and reporting

investigations, regulatory and external stakeholder updates and remediations[7] should be agreed.

- Controls to address the required protocols should cover, but not limited to, ownership, policies, systems, data security and protection for data sharing[8].

Implementing business process capabilities

Data management capabilities are relevant to each data sharing bank and embedded into existing business processes. In data sharing, such capabilities shall be expanded to include considerations for data sharing:

- **Data provenance:** For data elements shared under each data interoperability use case, key data documentation such as data inventory, data dictionary, data lineage and data quality metrics must be maintained.
- **Data ownership:** Individual data governance officers (DGOs) and data stewardship teams shall be clearly identified to facilitate data sharing for each use case, to drive accountability and benefits realisation.
- **Data integrity:** Categorise and protect data according to agreed standards for data sharing. Implement data standards and implement data quality monitoring to ensure that such standards are adhered to.

[7] See "Monitoring and continuous improvement" pillar on escalations and remediations of issues monitored

[8] See "Controls" pillar on the list of controls to facilitate data sharing

3. POLICIES AND PROCEDURAL DOCUMENTS

The policies and procedures around data sharing support the enablement of good data governance, quality and monitoring around its data sharing practices. Bank leaders shall promote data sharing, set out clear guidelines through documented policies and procedures to define the key documentation, roles and responsibilities and data standards. This demonstrates a clear mandate within the bank for data sharing.

Leadership commitment

- The sharing of data can occur across varied use cases and departments. Hence, in order to ensure the orderly management and control over sharing of data, roles and responsibilities must be clearly defined in relation to data ownership and governance, quality, data privacy and control over the data sharing initiatives.

Data sharing policy and procedures

- The objectives, scope of application and considerations for data sharing, among others, should be defined, documented and maintained in a formal policy and procedure.
- Minimum data documentation to be maintained includes data inventory, data dictionary, data lineage and data quality metrics.
- Policies and procedures shall include compliance with the domestic regulations and the counterparty bank's legal and regulatory requirements.

Data standards

- Data standards should be established and enforced to ensure that data protection, security, integrity and quality should be ensured throughout the data sharing lifecycle.
- Standard vocabularies and classifications are encouraged to improve consistency in the description of data and metadata (e.g. the Financial Industry Business Ontology (FIBO)).

Data sharing model

- Appropriate sharing model shall be selected and the associated rationales thereof documented. Possible options include[9] :
    - Bilateral - two entities agree to share their data, where sharing can be one-way or two-way. Trust is established directly between the two data sharing partners.
    - Multilateral - more than two entities agree to share data. Each entity in the agreement can take the role of the Data Importer, Data Exporter or both. This could be done via a data sharing service provider and may require a joint supervisory committee to ensure all parties act in bona fide good faith.
    - Decentralised - a marketplace model where authorised entities may share data bilaterally or multilaterally on an immutable trusted platform. This includes peer-to-peer and other distributed systems. These are designed to grant control over data access to a community of authorised participants.

[9] IMDA Trusted Data Sharing Framework - Understand Potential Data Sharing Models: https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

4. DATA INVENTORY

In the context of data sharing, data is shared electronically in a machine-readable format. Data inventory considerations relate to the categorization and protection of the data to be shared. It facilitates a sound understanding of the type of data held by the bank available for data sharing, the nature of the data including sensitivities (personal data vs generated data vs derived data, etc.), protection accorded and pre-conditions (such as consent, purpose, time-limit) to the use of such data.

Understanding the data
Due to the high volume and the various types of data a bank manages today, the process begins with the identification of the data that the bank is in possession of. As the bank evolves, there may be new types of data that the bank needs to handle. In such cases, the data inventory is updated as and when these new types of data are collected and shared.

A good data inventory can bring the following benefits:

- Clear and consistency definition of the data;
- Improve data discoverability; and
- Improve the value data sharing is intended to bring.

To populate the information regarding the data in possession, it is important for the business to answer the following questions:

- What type of data (e.g., transactional / personal / financial) is being collected and shared?
- Where is the authorised source of the data being stored?
- How can the data be accessed? What types of authorisations are required?
- Who is the intended recipient of the data?
- What is(are) the intended purpose(s) of the data importer?

Categories	Sub-categories	Illustrative Examples (Non-exhaustive)
Party Individual or legal entity that is a customer or has relationship with the bank.	• Legal entity • Individual • Related party	• **Personal data:** Name, address, date of birth, unique identification number • **Demographics:** Income, sector, nationality, incorporation country, occupation • **Contact information:** Phone number, email address, address
Account Registry of transactions; statement of business dealings or debits and credits; sum of money deposited at a bank.	• Customer account • Internal company account • General ledger (GL) account	• **Accounts:** Current/savings account, mortgage, corporate lending, global markets • **Statements:** Account balances, deposits, withdrawals
Product Product transaction and services provided to customer.	• Corporate/principal finance • Retail/consumer • Transaction banking	• **Transactions:** Amount, Currency, Instrument • **Payments:** Domestic and cross border: location, time, amount, currency • **Settlements:** Confirmations, margins,

	• Financial markets • Wealth management/private banking	terms, value amount, value date
Limit & Collateral Bank's appetite to extend a loan or facility, and asset or property pledged as security for a loan.	• Customer lending limit • Group lending limit • Account lending limit • Collateral • Guarantee	• **Scoring:** Internal and external ratings • **Limits:** Credit card, unsecured and secured lending (mortgage) • **Collateral:** Cash, securities
Risk and compliance data Risk measurement and control activities.	• Risk metrics • Finance metrics • Compliance • Technology	• Potential future exposure • Risk weighted assets • Value at risk • Gross operational losses
Reference data Commonly used across different systems for the purpose of categorising data.	• Market • Vessel • Country • Segment • Location	• **Currencies:** Currency code • **Industry standards:** ISO country code, SWIFT code • **Jurisdictions:** Area code, city code

Table 2: Examples of Categories and sub-categories of data in Banks

Source: Association of Banks in Singapore: Data Sharing Handbook for Banks and Non-Banks Data Ecosystem Partners: II Types of Data

Overarching considerations when categorising and protecting data

Banks have the flexibility to categorise their own datasets, appropriate to their respective needs. The areas for consideration listed here aim to assist in establishing relevant risk-based controls based on common data classification terms.

The data inventory shall be used to carry out risk assessment. A well-maintained data inventory includes up-to-date and detailed information regarding the data. This helps in performing risk assessment without delaying the data sharing lifecycle.

Controls should be applied based on the categorisation of dataset. Banks should keep the following considerations in mind when performing the impact and risk assessment to assign the appropriate tiers, and avoid over protection of datasets that may hinder the use of data for business purposes:

- Category: personal data (non-shareable data, profile data, generated data, derived data) vs non-personal data (anonymised vs public data)
- Data Type, Dataset,
- Ownership,
- Purpose,
- Security / Sensitivity,
- Archival of data / Destruction of data (Controls).

In the event of a data breach, the data inventory shall be used to support the development of breach notification plans, such as by identifying personal data implicated in the breach and the owners of the underlying programme or process that uses the personal data.

Classifying the data

- Data can be categorized into personal data[10] and non-personal data. These two categories of data – personal and non-personal data – can be further disaggregated per following table.

[10] Personal data, also known as personally identifiable information, is any information related to an identifiable person.

Class of data	Sub-class of data	Characteristics	Examples
Party data	Non-shareable data	Unique to customers	Passwords, biometric data
	Profile data	User consent is required for sharing	Name, date of birth, address
	Generated data	Digital trails generated by the online activities of a customer; consent is required too	Transactions e.g. Payment history, card transactions
	Derived data	Developed by service providers through the mapping of generated data together with other attributes, some form of consent is required	Total Investable Assets, Total Spending Habits
Business data	Anonymised data	Do not map to the identity of data subjects	Aggregated data with no personal identifiers
	Public data	Consent is not required for assembling these data sets	Bank annual report

Table 3: Classifications of personal and non-personal data

- The data inventory shall contain key information such as ownership, purpose, sensitivity level and types of controls, to better understand the data at hand.

5. IMPACT/RISK ASSESSMENT

The bank must leverage its risk management framework to assess the risks of data sharing, potential impacts and take actions / control measures to reduce such risks.

Risk assessment and monitoring

- Perform risk assessment for identified risk factors, considering factors such as the type, sensitivity and criticality of the data. Data sharing risks may include:

Data Privacy	Data Control	Data Quality
Risk of unauthorised / inappropriate disclosure/personal data breaches. For information to be private and confidential, the access to some information needs to be restricted because it could harm interests of the stakeholders.	Loss of control over data when it moves outside of the bank's information system. Data holders lose their capabilities to control how data are being used/re-used.	Risk to information quality / corruption and unavailability. For information to be useful and serve the purpose, it must be accurate, complete and available on a timely basis.

- Risks identified should be treated (e.g. avoid, reduce, transfer, share risk, etc.) to minimise the risk.
- Assess the residual risks and conduct a risk acceptance process to obtain management acceptance.
- Establish the appropriate risk controls, monitoring and reporting mechanisms, and risk remediation plans.

Impact assessment

The impact assessment of a data breach is crucial to any data sharing initiative. It is a formal way of evaluating and documenting the likelihood and consequences in the event of a data breach and allows the management to undertake the necessary controls and continuous enhancements to these controls in order to minimise such an impact.

- Establish guidelines and thresholds to evaluate the significance / magnitude of data compromise impact on customers and the business of the data importer and/or exporter.
- Where personal data is being transferred, consider if a Data Protection Impact Assessment (DPIA)[11] is required.

[11] A data protection impact assessment (DPIA) is a privacy-related impact assessment whose objective is to identify and analyse how data privacy might be affected by certain actions or activities.

6. CONTROLS

A control is relied upon to prevent errors from occurring during data collection, transmission, use and/or disclosure processes (preventive controls) or to detect and correct errors that may have occurred in any of these processes (detective controls). The risk-based controls implemented are commensurate to the potential
impact of the data loss / breach being compromised.

General controls over all data

- Establish and implement input and output checks to maintain data integrity and quality and minimise the risk of potential misuse.
- Implement data security controls such as encryption, obfuscation and tokenisation over the transmission of the data to minimise loss in the integrity of the data, unauthorised changes to the data and misuse of data.
- Formal documentation of data restoration and disposal processes should be performed so that data can be recovered or rendered irrecoverable, where necessary.
- Implement internal audit procedures as an independent assurance means to ensure that the desired controls are put in place adequately.

Specific controls over personal data

- All personal data must have a register of authorised sources and authorised users to be maintained by both the Data Exporter and in the Data Importer.
- The sharing of personal and confidential data must be recorded, auditable and controlled so that in the event of request by the Data Subject on the use of his/her personal data,, this information may be provided even when it is shared across borders.
- Such controls must be in accordance with jurisdictional laws and any further relevant privacy and security policies.
- Security controls and mechanisms must be enabled for personal and confidential data and recorded in a data inventory.
- Personal data retention, archiving, and purging must be managed according to the agreed retention schedule and at any other times as may be changed during sharing.
- Controls over personal data can include privacy preservation techniques such as masking of personal data, anonymisation, or aggregation, depending on the best approach for each data sharing use case.

7. MONITORING AND CONTINUOUS IMPROVEMENT

Ongoing monitoring is critical to manage risk of breaches and/or detect non-compliance. The extent of monitoring required will vary according to the level of sensitivity of the data. Continuous improvement comprises key activities such as monitoring, measurement, analysis and evaluation to keep the various components of the Framework up-to-date and optimised.

Key design activities

- Determine how to monitor the adherence to agreed metrics and minimum data standards.
- Define the acceptable threshold limits for the defined metrics and data standards.
- Consider how emerging risks on data compromise during sharing can be monitored on an ongoing basis.
- Specify in the event breaches are identified, how should these be reported, and access managed to ensure that such risks are reduced to an acceptable level as soon as possible.

Key execution activities

- Periodically review the design of the process for assigning categories to datasets (see "Data Inventory") and performing risk assessment (see "Impact / Risk Assessment").
- Periodically review controls, contingency plans and technology implemented, evaluate their effectiveness to mitigate emerging risks identified and remediate where necessary.
- Be continuously updated on developments in data sharing best practices in order to engage in continuous enhancements.
- Continuously monitor for any changes that may arise on legal and regulatory obligation and take all necessary measures to ensure they remain compliant to the revised legal and regulatory obligations.

8. ADVOCACY

The culture of trust is cultivated from information flowing freely and safely across borders and across financial institutions. It requires support at the highest levels to promote data-sharing and raise awareness of its benefits. With that as a foundation, banks can then pursue a culture of information-sharing and cross-fertilisation at the operational level. This requires good communication and advocacy efforts from management to all staff levels.

Tone from the top

- Obtain executive sponsorship to promote a data-driven culture and set the "tone from the top" that data is an asset to be maximised with adequate controls in place.

Training and communication

- Provide regular training for employees to enhance data literacy across the bank, awareness of data privacy rules and promote trust in data sharing.
- Establish and communicate the importance of data privacy and security, including potential consequences if data is compromised. Personal accountability towards data privacy is to be established across the bank.
- Delineate clear roles and responsibilities and provide training and assessment to employees to ensure that they have sufficient skills and authority in data sharing.
- The complexity and expertise required to address different areas of risks often leads to a silo or a narrow approach. For example, legal and confidentiality requirements, supervisory and statistical concepts/methodologies, statistical techniques, information and communication technology and dissemination tools all require different skills from different organisational teams. Efforts are required to establish a collaborative culture of working together with openness.

Organisational forum and proof-of-concepts

- Establish an organisational forum for ecosystem engagement, exchange of high value data sharing opportunities, sharing of best practices and showcase success stories to promote data interoperability.
- Trust in data sharing use case(s) may be further established using a proof-of-concepts/sandbox environment for parties to test the technical feasibility of ideas in a fail-safe environment.

9. TECHNOLOGY

Technology enables banks to simplify the mechanics of data sharing by ensuring technical operability, common system standards and considering appropriate emerging technologies.

Technical interoperability

- Consider the principles of technical operability (i.e., frequency, volume, speed, sensitivity, affordability) when making technology decisions.
- Evaluate and document the rationale for selecting the technical delivery mode for data sharing. Common examples include Application Programming Interfaces (APIs), open banking ecosystem[12], distributed ledger, remote access, removable storage / media, etc.
- Data in motion: Implement and document appropriate security measures to safeguard data integrity, such as encryption and tokenisation. Where data is to remain at rest, consider secure computation techniques such as homomorphic encryption and multi-party computation.
- Implement and document appropriate data masking measures to safeguard privacy, such as data pseudonymisation.
- Adopt open standards where applicable.

System and data standards

The system should meet the following five standards:

(i) purpose limitation	(ii)minimisation data	(iii) retention restriction	(iv) use limitation	(v) operational resilience
i.e. ensure that the purpose for which data are being shared is described in clear and specific terms	i.e. share only as much data as are strictly necessary to achieve the stated purpose	i.e. ensure that data are not shared for longer than required to achieve the stated purpose	i.e. ensure that data are used only for the purpose for which they were shared	i.e. ensure that data are secure, and the overall system is resilient to unauthorised access

Source: BIS Papers No 124 – 4.b The conditions for data-sharing

Digital consent is usually a common legal basis for data processing. To ensure ease collection and maintenance of such consents, such systems are built around the so-called BIS ORGANS principles

Open require the use of open, interoperable standards for the sharing of data	**Revocable** enable the revocation of consent once provided by the data subject	**Granular** allow for consent to be provided in granular fashion just before data are shared.
Auditable give data subjects the right to audit data-sharing transactions.	**Notice** recognise consent as a requirement for processing and sharing of data and require a notice of consent prior to collection, processing and sharing of data.	**Secure** impose data security obligations on data controllers.

Source: BIS Papers No 124 – 4.c ORGANS principles

Emerging technologies

To ensure that the banks take advantage of the latest emerging technologies to further safeguard and

[12] Open banking (aka open financial data) allows an expanding universe of players—both financial and non-financial—to access customer accounts and data in order to offer new products and services (all contingent on customer consent). The ecosystem refers to the interconnected system to enable open banking: https://www.mckinsey.com/industries/financial-services/our-insights/financial-services-unchained-the-ongoing-rise-of-open-financial-data

enhance their data sharing practices, banks must continuously remain informed of latest advances and review the potential of deploying such technologies to new or existing data sharing initiatives.

- Review and explore technological developments such as emerging privacy preservation techniques, and privacy enhancing technologies (PETs) to enhance the data sharing process and safeguard data against compromise.
- To mitigate security risks and regulatory consequences, consider the use of 'sandboxes' – a segregated testing environment for new software or applications, with limited or no connection to the rest of a network.

The Way Forward

D. The Way Forward

In the financial services sector, increased data collaboration supports economic growth and the development of innovative financial services and benefits risk management and compliance programs. This greatly benefits ASEAN to be a fertile ground for the development of digital banking. This is especially so with the ASEAN consumers' tech-savviness that has created opportunities for banks to deliver new innovations and leap ahead. In order to move towards the new age of digital banking, each bank would need to reinvent itself to stay relevant.

This can be supported by increased data collaboration and connectivity where banks can develop innovative solutions to redesign processes to achieve radical gains in productivity and leverage new strengths in data analytics to drive efficiencies and effectiveness. With digital banking, banks will increasingly both acquire new customers and interact with ongoing customers through digital ecosystems and increased data collaboration across ASEAN can drive changes in the banks' business models and technology architecture.

Data collaboration will become increasingly important in unlocking the value of data through partnerships with the industry, regulators and others within the financial ecosystem. To achieve this, it is essential for banks in ASEAN Member States to understand the legal, regulatory, processes and other capabilities underpinning cross-border data sharing within ASEAN. This ASEAN Banking Interoperable Data Framework provides the recommended best practices and equips banks with understanding the needful requirements for a successful implementation.

Acknowledgements

E. Acknowledgements

The ASEAN Banking Interoperable Data Framework ("IDF") was commissioned by the Cooperation in Finance, Investment, Trade and Technology (COFITT) Committee of the ASEAN Bankers Association (ABA). The ABA IDF Taskforce was formed to facilitate data sharing for ASEAN member banks to better meet customers' financial needs in today's digital economy, while upholding customers' trust in banking institutions to protect the privacy of their information.

The Handbook was crafted with the inputs of the ABS IDF Taskforce members from:

- The Brunei Association of Banks
- The Association of Banks in Cambodia
- PERBANAS (Indonesian Banks Association)
- Lao Bankers' Association
- The Association of Banks in Malaysia
- Myanmar Banks Association
- Bankers Association of the Philippines
- The Association of Banks in Singapore
- The Thai Bankers' Association
- Vietnam Banks' Association

In addition, the Handbook was completed with the strong support of:

- The Enterprise Data Management Council

We would also like to acknowledge the guidance from our ASEAN regulatory stakeholders, banking associations, specifically the ASEAN Working Group on the Digital Data Governance (WG-DDG), Working Committee on the ASEAN Banking Integration Framework (WC-ABIF) and Working Committee on the ASEAN Payments and Settlement Systems (WC-PSS).

Finally, we would like to thank all organisations and individuals not otherwise mentioned, for their active participation in the creation of the Handbook.

Glossary

F. Glossary

Data interoperability
refers to the ability to access and process data from multiple countries in a safe and secured manner, and which complies with legal and regulatory requirements of the sharing countries.

Data localisation

refers to data that is subject to being withheld within the ASEAN Member State which it is collected in, based on the local laws and governance structures of that Member State.

Personal data

is data about an individual who can be identified directly from that data or derived from the pieces of information which the bank has access to.

Data inventory

Is the categorization of the data to facilitate a sound understanding of the type of data held by the bank available for data sharing, the nature of the data including protection requirements due to sensitivities (personal data vs generated data vs derived data, etc.), protection accorded and pre-conditions (such as consent, purpose, time-limit) to the use of such data.

Appendix

G. Appendix

High level summary of regulatory compliance for considerations of ASEAN Member States as of November 2022:

Country	General Regulations Established	Data Localisation Required?	Cross-Border Data Sharing Disallowed?	Personal Data Privacy Requirements Defined	Data Management Requirements Defined	Data Security Requirements Defined
Brunei	Banking	No	No	Draft Data Protection Policy	Guidelines	Guidelines
Cambodia	Banking	No	No	Draft Data Protection Guidelines, Sub-decree	Guidelines	Guidelines
Indonesia	Banking Infocom	Yes	No	PDPA still in draft (*Currently reliant on OJK Regulations*)	No	Laws
Laos	Banking Law on Electronic Data Protection	No	No	PDPA still in draft (*Currently reliant on* *Law on Electronic Data Protection*)	Law on the Protection of Electronic Data,	Instructions
Malaysia	Banking Personal Data Protection Act (PDPA)	No	No	PDPA	Policy, Standard, Code of Practice, Guidelines	Policy, Code of Practices
Myanmar	Banking	No	No	Nil	High Level Instructions	Nil
Philippines	Banking Data Privacy Act (DPA)	No	No	DPA	Guidelines	Acts
Singapore	Banking PDPA	No	No	PDPA	BCBS 239	Act, Guidelines
Thailand	Banking PDPA	No	No	PDPA	Policy Statement	Notifications, Framework, Guiding Principles, Guidelines

Vietnam	Banking	Yes	No	Draft Personal Data Protection Decree (PDPD)	Nil	Acts

ASEAN
Bankers Association

Copyright 2023 — ASEAN Bankers Association

This publication gives a general introduction to contractual terms and conditions and templates that can help identify key issues when transferring personal data across borders.