ASEAN Bankers Association

ASEAN Banking Interoperable Data Framework (IDF)

Safe and secured cross-border flow of data

Guidance Document

THE BRUNEI ASSOCIATION OF BANKS

สมาคมธนาคารแห่งกัมพูชา
THE ASSOCIATION OF BANKS IN CAMBODIA

PERBANAS
INDONESIAN BANKS ASSOCIATION

สมาคมธนาคารลาว
LAO BANKERS' ASSOCIATION

PERSATUAN BANK-BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Myanmar Bankers Association

BANKERS ASSOCIATION OF THE PHILIPPINES

abs
The Association of Banks in Singapore

สมาคมธนาคารไทย

VNBA

Version 1.0 November 2022

Contents

Introduction

This Guidance Document is intended to be read in conjunction with the ASEAN Banking Interoperable Data Framework (Framework). It contains answers to common questions on data interoperability and implementation that readers may have while reading the Framework. It aims to:

- Provide additional details on the principles and concepts laid out in the Framework
- Reference industry best practices
- Provide references to open data standards that may be applicable depending on the use case for data collaboration
- Illustrate how the concepts may be applied through worked examples
- Detail guidance on the implementation and operationalisation of the Framework

This Guidance Document is organised in alignment with the pillars described in the Framework and provides relevant definitions, implementation and operationalisation considerations. It should not be construed as legal advice and readers are encouraged to seek appropriate legal counsel in relation to their legal or regulatory obligations when engaging in data interoperability and collaboration activities.

General

2. What is data interoperability and how does it differ from data collaboration?

Data interoperability in the Framework refers to the ability of data to be integrated and used by different organisations across borders and is concerned with the processing and interpretation of received data. This may or may not involve the actual transfer of the data itself. Data collaboration is the ability to distribute the same sets of data resources with multiple users or applications while maintaining data fidelity at the basic level. To ensure data collaboration is successful among the parties, data interoperability is key.

3. Who is the owner of ASEAN Banking Interoperable Data Framework?

The owner of the Framework is the Cooperation in Finance, Investment, Trade and Technology (COFITT) Committee of the ASEAN Bankers Association (ABA). As the owner, the COFITT Committee will be responsible for ongoing revisions to the Framework to ensure its fit for purpose as technology, business models and regulations evolve.

4. Is data in physical hardcopy documents within the scope of the ASEAN Banking Interoperable Data Framework?

No, the scope of the ASEAN Banking Interoperable Data Framework relates only to digital and/ or digitalised data that is stored in a structured and machine-readable format. Unstructured data (e.g., PowerPoint deck, scanned documents and physical hardcopy) is not in the scope of this Framework.

5. Is the ASEAN Banking Interoperable Data Framework legally binding and does it require regulatory/ compliance checks?

The ASEAN Banking Interoperable Data Framework is a voluntary and non-binding principles-based framework established on recommended practices on data interoperability for the banking industry within ASEAN Member States. Whilst it is voluntary and non-binding, member banks engaging in any form of data collaboration are strongly encouraged to adhere to the guidance and principles embedded within the Framework.

The Framework has incorporated latest regulatory and legal requirements at the point of publication. However, this should not be construed as conclusive regulatory and legal advice. Hence, ASEAN Member States are advised to perform their independent compliance checks to ensure conformance to latest updated regulatory developments amongst the sharing countries.

6. Will banks in ASEAN Member States be given flexibility in implementing this ASEAN Banking Interoperable Data Framework?

Yes, the ASEAN Banking Interoperable Data Framework is expected to facilitate such cross-border data flows between participating ASEAN Member States. Cross-border data collaboration is voluntary but highly encouraged. The ASEAN Banking Interoperable Data Framework takes into account the different levels of maturity and local laws within the ASEAN Member States, and provides ASEAN Member States with guidance on whom they may share data with, the types of data that may be shared, and how they may share such data and the binding conditions under which they may share. Each ASEAN Member State may then assess their participation in the ASEAN Banking Interoperable Data Framework when they are ready to do so within their domestic laws and regulations.

7. Can banks use the ASEAN Banking Interoperable Data Framework for data collaboration with ecosystem partners?

The initial scope of application of the ASEAN Banking Interoperable Data Framework is on data interoperability within the banking industry amongst the ASEAN Member States. Data collaboration with ecosystem partners will be covered under the broader umbrella of the ASEAN Data Management Framework.

For the purpose of clarity, ecosystem partners refer to entities whom banks partner with for mutually beneficial outcomes - e.g., insurance companies, telecommunication providers, vendors, etc.

8. Does the ASEAN Banking Interoperable Data Framework include industry best practices, international standards and frameworks?

Yes, the ASEAN Banking Interoperable Data Framework adopts recommended practices from the following:

a. Best industry practices from Enterprise Data Management Council's DCAM framework e.g., Cloud Data Management Capabilities (CDMC) Framework that highlights the 14 controls for the management and protection of sensitive data in a cloud environment

b. Best industry practices from World Economic Forum's Cross-Border Data Collaboration Roadmap

c. Considerations and practices from the ASEAN Data Management Framework

d. Local member country's data collaboration frameworks, where applicable

e. ISO270001 (Information Security Management) that prescribes the standard practices to

protect and govern the security of the data

Where relevant, the ASEAN Banking Interoperable Data Framework referred to these standards/ frameworks to incorporate data integrity, quality and uniformity considerations to promote the interoperability of data.

9. What are the expectations out of each ASEAN Member States to implement this ASEAN Banking Interoperable Data Framework?

Each ASEAN Member State should encourage their banking institutions to adopt this Framework when developing their data sharing processes, policies and agreements. Where data management guidelines have not been established within the local states, they may consider adopting the principles in this Framework as a general guidance.

10. Where can a bank find prescriptive guidance in the ASEAN Banking Interoperable Data Framework?

The ASEAN Banking Interoperable Data Framework is principles-based and is not intended to be prescriptive in order to allow flexibility for each sharing party to collaborate based on the use case and their existing business operating models. This Guidance Document is meant to provide further operational guidance.

11. Will there be regulatory checks on the ASEAN Banking Interoperable Data Framework?

No, the objective of the ASEAN Banking Interoperable Data Framework is to create a cross-border flow of data without imposing regulatory requirements to override existing policies for interoperability and data regulations that may exist in the member countries.

12. Is the same level of rigour in governance and controls recommended in the ASEAN Banking Interoperable Data Framework consistently applied in all use cases?

No, the level of rigour applied will depend on the type of data shared and the risk and materiality of the use case. Every bank should apply judgement to determine the most appropriate level of governance and controls as agreed between the sharing parties.

13. How would the ASEAN Banking Interoperable Data Framework interfere with or impede the banks in countries which have existing bilateral arrangements for cross-border payments and those which are planning to interconnect with their instant payment systems?

The ASEAN Banking Interoperable Data Framework aims to support and expedite any such collaborative initiatives, including but not limited to cross-border payments. For countries where bilateral arrangements have been agreed upon, the existence of the ASEAN Banking Interoperable Data Framework does not interfere with the arrangements. For countries aiming to implement such initiatives, the ASEAN Banking Interoperable Data Framework can be used to align data standards, controls, governance and quality.

1. Legal and Regulatory Compliance

1. **Given the many regulatory considerations, data protection requirements and challenges like data sovereignty, how can the ASEAN Banking Interoperable Data Framework help banks address and meet their legal and regulatory obligations?**

   The ASEAN Banking Interoperable Data Framework lists the key legal and regulatory considerations for data collaboration, including determining what data can be shared and its purpose, protection measures, and obligations of data importers and exporters. Local regulatory compliance considerations such as data privacy, data localisation and protection considerations across countries are summarised in the Table of Regulatory Requirements for ASEAN Member States in the Appendix of ASEAN Banking Interoperable Data Framework.

2. **Is it mandatory to adopt the full ASEAN Model Contractual Clauses (ASEAN MCCs)? Can we be allowed to adapt to our local version?**

   The ASEAN MCCs are a proposed set of contractual terms and conditions incorporating all the common data collaboration considerations. It is meant to address the lack of a standardised agreement within the industry for data collaboration that has resulted in highly complex and lengthy documentation, bespoke clauses, and terms and conditions. Adoption of this is voluntary but encouraged, especially where this legality is still less developed in some ASEAN Member States.

3. **Does compliance to ASEAN Banking Interoperable Data Framework automatically entitle an organisation to be certified under APEC Cross-Border Privacy Rules (CBPR) System? How does one get certified?**

   The APEC CBPR provides certification to banks that comply with internationally recognised data privacy protections. Compliance with the ASEAN Banking Interoperable Data Framework requirements provides banks in the ASEAN Member States with the prima facie demonstration of capabilities to comply with the APEC CBPR. However, it does not entitle a bank to be automatically certified given its additional need for an Assessment Body (AB) to act as an independent body to assess that their data protection practices conform to the APEC CBPR requirements.

4. **How may the individual's personal data privacy considerations in each country be adhered to, given that the rate of enactment into law is different across the countries?**

   The ASEAN Banking Interoperable Data Framework has considered the various personal data protection requirements and the state of development of these in respective countries. Most of the countries have some form of data privacy requirements that have been either enacted, or in the process of enactment or incorporated into an existing legislation. The specific data privacy compliance requirements and penalties have been collected and the latest responses from the country regulators (as of August 2022) are found in its Appendix.

   Under the Legal and Regulatory Compliance pillar, we have taken the above into consideration and required that *Data is handled in compliance with local regulations (and the GDPR if applicable) and used in accordance with the prescribed purpose(s).* Data sharing parties are strongly encouraged to perform their independent checks on the latest status of regulatory updates into their data sharing arrangements.

5. **How does the ASEAN Banking Interoperable Data Framework address the risk of data breaches in the sharing process?**

The ASEAN Banking Interoperable Data Framework has considered the various personal data protection requirements and the state of development of these in respective countries. Most of the countries have some form of data privacy requirements that have been either enacted, or in the process of enactment or incorporated into an existing legislation. The specific data privacy compliance requirements and penalties have been collected and the latest responses from the country regulators (as of August 2022) are found in its Appendix.

Under the Legal and Regulatory pillar, we have taken the above into consideration and required that *Data is handled in compliance with local regulations (and the GDPR if applicable) and used in accordance with the prescribed purpose(s).* Data sharing parties are strongly encouraged to perform their independent checks on the latest status of regulatory updates into their data sharing arrangements.

2. Governance and Oversight

1. **Beyond regulatory requirements, what are the other considerations included in the ASEAN Banking Interoperable Data Framework to help banks collaborate with data?**

   The ASEAN Banking Interoperable Data Framework is aligned with regulatory requirements and is also designed and baselined with consideration of industry leading practices, such as recommended data standards, components to be maintained within the data inventory and monitoring controls for data collaboration within ASEAN.

2. **What happens if my bank does not have the same stakeholders as listed in the table of roles and responsibilities?**

   The listed stakeholder roles and responsibilities are illustrative. Each organisation may assign different designates or stakeholders to perform similar roles or multiple roles.

3. **What is the key difference between being accountable and responsible across the various stakeholders in a data collaboration arrangement?**

   In accordance with the COSO RACI Matrix, Responsible refers to person or stakeholder who is tasked to perform the work. Accountable, on the other hand, refers to person or stakeholder who assumes ownership of the work. Please refer to the COSO RACI Matrix for further detailed guidance.

4. **Should each ASEAN Member State establish a new national Data Management Function to oversee data collaboration initiatives?**

   No, there is no requirement for a new National Data Management Function to be established in this ASEAN Banking Interoperable Data Framework or the associated ASEAN Data Management Framework. In most circumstances, banks may leverage established governance and control frameworks/ structures for data collaboration if they have been assessed to be adequate for the purpose. The ASEAN Banking Interoperable Data Framework provides a baseline reference to implementing data collaboration arrangements, organisations may enhance the recommended guidelines deemed necessary.

5. **Is it mandatory to appoint an independent assessment body to attest adherence of defined data governance standards, policies and other stipulations within the data sharing agreement?**

   No, however it is strongly recommended to attest adherence to the legal obligations defined within the data sharing agreement. This independent assessment body can be assigned internally or externally, in the absence of which, the onus of proof is on the banks that they have complied with the requirements. Consideration should be based on the suitability (i.e. degree of independent and impartiality) and availability of expertise to perform the role.

6. **Is there an independent body in the ASEAN network to regulate and monitor the compliance to ASEAN Banking Interoperable Data Framework?**

   No, there is no regional independent body at this point to perform this monitoring role. The Framework is not intended to be a regulation or legislation but provides recommended practices to be adopted when banks intend to collaborate on data. As such, monitoring will only be based on the mutual contractual agreement between the data exporter and the importer, based on the ultimate data sharing terms and conditions agreed between these parties and adopted into the

legal agreement.

3. Policies and Procedures

1. **How do the parties within the bilateral agreement limit the use of data that defined in the bilateral agreement and enforce this?**

   The limitations on the use of the data (including the period of its use) is recommended to be clearly and expressly specified in the data sharing agreement. The parties of the bilateral agreement are at liberty to discuss and agree the purpose, extent of the use and time period to which the data should be retained after use. Under the Governance and Oversight pillar, the Framework also recommends the deployment of an independent assessment body (which can be an internally assigned body) to attest to the adherence of such requirements and to report any exceptions and breaches.

2. **What are the common challenges related to data collaboration and interoperability and how would establishing internal policies and procedures address such challenges?**

   Common challenges include:

   a. Data discovery and understanding challenges due to availability and quality of metadata. Data discoverability is a highly protracted process due to lack of availability, quality and standardisation of data dictionaries and glossaries.

   b. Managing onward data use outside of the agreed/ primary use case is a concern and a trust factor. Enforceability, assurance and auditability of data collaboration arrangements is a major concern and key to building early trust.

   c. Establishing a mutually beneficial/ equitable data collaboration partnership may pose problems due to lack of clarity on what data is available and how to derive mutual benefits.

   The ASEAN Banking Interoperable Data Framework policies and procedural documents pillar establishes key procedural considerations and standards to effect data collaboration as aligned to regulatory and legal requirements throughout the data lifecycle. Incorporating these within the banks would allow the banks to be readily aware of what data they can share, and how they can share without comprising on legal standards to ensure mutually beneficial outcomes. This will shorten the pre-sharing capability assessment and uplift required to facilitate data sharing.

3. **What are the recommended standards that can be referred to for the policy setting and procedure development process?**

   The below are some examples of widely adopted global industry standards within the banking industry:

   a. The Financial Industry Business Ontology (FIBO)

   b. ISO 9362 Standards - Business Identifier Code (BIC)

   c. ISO 13616 Standards - International Bank Account Number (IBAN)

   d. ISO 10383 Market Identifier Code (MIC)

   e. ISO 17442 Legal Entity Identifier (LEI) reference standards

   f. The DAMA Data Management Body of Knowledge (DAMA-DBOK) provides standard

industry view of data management functions, terminology and recommended practices

4. Data Inventory

1. **What is the difference between data discovery and system inventory?**

   Data discovery focuses on the data interoperability while the bank should have a full system inventory which addresses the data management and internal requirements.

2. **What additional information can be captured in the data inventory to facilitate data interoperability?**

   The following table provides some examples and descriptions of key data inventory fields:

Notes	Data Fields	Example
Illustration from ASEAN Data Management Framework	Purpose	Analysis of item costing
	Data Owner	Finance
	Data Type	Business data
	Data fields	Item descriptions and cost
	Dataset	Procurement transactions
	Source Location (System)	SharePoint
Additional Information for Data Interoperability	Recipient(s)	Outsourced Finance Teams
	Recipient Country(ies)	Malaysia, Thailand
	Disclosure Purpose	To process transactions
	Category	Generated data
	Sensitivity	No
	Security	Encryption, Whitelisting
	Archival of Data	> 3 years data would be moved to Secured Vault
	Destruction of data	Hard Deletion of > 7 years data from Secured Vault
	Sharing Platform	SFTP Server

3. **Where should the data be hosted and how do local restrictions impact the hosted location?**

   Hosting of the data is situational, and the 3 scenarios are indicated below:

   a. No Data Transfer: No data hosting is required, and this will be managed through data access.

   b. Direct Transfer: Data hosting details and requirements will be specified in the data agreement, subject to data transfer restrictions that may apply locally. Please refer to the Appendix of the Framework for a list of countries where data transfer restrictions may exist.

   c. Multilateral Transfer: Data hosting details and requirements will be specified in all the data agreement between the involved parties. Care should be taken when considering the location of such hosting sites to minimise risks of breaching data localisation laws, and existing legislation on data management and data privacy. Please refer to the Appendix of the Framework for a list of countries where data transfer restrictions may exist.

   Each data exporter and importer should comply with their local restrictions which may differ from country to country. They should have a receiving hosting site for the data importer and vice versa for the exporter.

4. What is data minimisation, and should we consider it?

Data minimisation refers to sharing only as much data as strictly necessary to achieve the stated purpose. This should be considered and controlled by the banks. Banks should consider data minimisation in data collaboration, including:

a. Be clear about the purposes the data is being shared

b. Share the minimum amount of data needed for those purposes

c. Store that data for the minimum amount of time the data is required for

5. Do we need to revisit consent each time before sharing the data?

In general, once consent is provided, organisations are not required to request for consent repeatedly each time personal data is used or shared, unless there are changes to what data is used and for what purpose. The existing consent must be for (a) a specific purpose and (b) a specific period.

5. Impact/ Risk Assessment

1. **What impact categories should be considered under impact assessment to facilitate data interoperability?**

   There are four primary impact categories to be considered:

   a. Financial - Risks affecting the financial processes of the company (e.g., accounting and reporting, tax, etc.)

   b. Strategic - Risks affecting achievement of the strategic objectives of the company (e.g., governance, strategic planning, major initiatives, etc.)

   c. Operational - Risks affecting the operations of the organisation (e.g., sales and marketing, supply chain, etc.)

   d. Compliance - Risks affecting the company's compliance with regulatory requirements (e.g., legal, code of conduct, etc.)

2. **How should an impact level matrix look like?**

   The following table provides some examples and descriptions of impact level matrix:

Impact Category	Financial Impact	Operational Impact	Reputational Impact	Legal/ Compliance Impact
Tier 1	Compromise of information to cause significant harm/ damage towards operations, organisations and individuals			
Tier 2	Compromise of information to cause moderate harm/ damage towards operations, organisations and individuals			
Tier 3	Compromise of information to cause limited harm/ damage towards operations, organisations and individuals			

6. Controls

1. **What is deemed personal data? What are the recommended technology controls over personal data?**

   Definitions of personal data can differ between jurisdictions. For the purposes of the ASEAN Interoperable Data Framework, personal data refers to data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access. Examples of personal data are name, address, and date of birth.

   Controls required over personal data include consent, purpose limitation, correction of data, accuracy, protection and retention. There are various types of metadata management tools that can support the above. For protection of personal data, recommended technology controls include privacy preservation techniques - pseudonymisation, hashing, anonymisation, minimisation, aggregation and use of digital twin.

   The ABS Data Sharing Handbook - *What is Sensitive Data?* section provides a good view of how these privacy-preserving mechanisms work.

2. **What non-data related control(s) should banks consider facilitating data collaborations?**

   The banks should consider technology and legal and regulatory controls.

   Technology controls may include choice of technologically secured platforms, management of in-house security for infrastructure, standardisation of content format and structure, use of cryptography, application of privacy preservation techniques and user access management.

   Legal and regulatory controls may include data ownership, tax implications, warranties and breach notifications.

7. Monitoring and Continuous Improvement

1. **Would it be more ideal to implement monitoring and control mechanisms after development of the ASEAN Banking Interoperable Data Framework within my organisation since this is for continuous improvement?**

   It is strongly recommended that for a more resilient end-to-end process, monitoring and control mechanisms should be implemented and embedded into the organisational workflow and processes.

2. **To ensure that we adhere to the minimum data standards, what are some of the recommended performance metrics that can be implemented?**

   Some of the performance metrics (not exhaustive) for the ASEAN Banking Interoperable Data Framework pillars:

   a. Legal and Regulatory: Number of breaches, Percentage of incidents caused by third parties, Number of regulatory compliance Issues opened

   b. Policies and Procedural Documents: Number of exceptions raised, Number of policy or procedural compliance issues opened

   c. Data Inventory: Distribution of types of data and countries transferred, Percentage of expired data not destructed

   d. Impact/ Risk Assessment: Number of DPIA performed, Number of risks not treated timely, Number of overdue remediation plans

   e. Controls: Number of controls deemed inadequate, Number of breaches due to lack of controls

   f. Advocacy: Number of data literacy programs rolled out, Passing rate of each data literacy programs

   g. Technology: Number of open standards adopted, Number of sandboxes used, Distribution of privacy preservation techniques and privacy enhancing technologies (PETs)

8. Advocacy

1. **Advocacy is one of the key enablers identified by the ASEAN Banking Interoperable Data Framework. Why is the focus organisational as opposed to being industry-centric?**

   All forms of advocacy need three tiers - one is at the core level within an organisation, and another, for collaboration within the industry locally and finally across countries. This Framework focuses on the most fundamental layer of advocacy which is at the organisational level.

   Banks have direct control over advocacy at their organisational level as this is within the control of management and the staff. This forms the primary basis of ensuring receptivity to data collaboration, understanding its benefits and create an internal buy-in to uplift data capabilities and infrastructure to be ready for exporting or importing data.

2. **What are some metrics and Key Performance Index (KPIs) that a bank can adopt to measure the levels of data literacy and awareness of data privacy rules?**

   Examples include but are not limited to:

   a. Number of employees passing related trainings or receiving certifications

   b. Number of data breaches and trend over time

   c. Employee's understanding of data provenance and lineage

   d. Mean time to data issue discovery

   e. Mean time to data issue resolution

3. **How may an organisational forum on advocacy benefit the wider ecosystem engagement?**

   Such forums allow the ecosystem to showcase success stories and promote new case studies. It promotes transparency and allow ecosystem partners to exchange feedback and experiences and provides confidence that ASEAN member state banks have minimum baseline data capabilities that do not just restrict data sharing within ASEAN, but outside of ASEAN too. This promotes trade and digitisation outside of ASEAN and underpins economic growth of our ASEAN Member States.

9. Technology

1. What are the standards for data encryption?

There are two primary types of encryption - symmetric key encryption and public key encryption. Standards applicable to both types of encryption include:

a. Encrypted files should not be indexed

b. Certificates and private keys for recovery agents should be stored on separately secured media objects

c. Federated Information Processing Standards Publication 140 (FIPS-140) compliant encryption algorithms should be used

d. Secure channel traffic should be encrypted and signed

e. Two forms of key recoveries should be available to users of the system

If the bank is not able to meet any of the above standards or require further guidance, the bank should contact its national cyber security agency for references and guidance.

2. Does the ASEAN Banking Interoperable Data Framework require a standardised technological/ infrastructural platform to facilitate data interoperability?

There are several platforms currently that have been considered in the development of the ASEAN Banking Interoperable Data Framework. While the Framework does not mandate the use of any specific platform for data interoperability, so long as the outcomes are aligned with respect to the Framework principles. This also ensures that the Framework remains technology-agnostic and practical.

3. What are the examples of technical data interoperability open standards we can use?

Open standards provide a common vocabulary for exchange of data between organisations and systems using common formats and shared rules. In general, there are four levels of data interoperability: foundational, structural, semantic and organisational.

a. Foundational

- ISO 8000 (Data Quality): Defines characteristics of information and data that determines quality and provides method to measure data quality
- ISO 27701 (Privacy Information Management System): International standards for data privacy
- ISO 27001 (Information Security Management System): Addresses information security within an organisation to ensure data accuracy, availability and data access rights
- ISO 20614 (Information and Documentation): Defines data exchange protocol for interoperability and preservations
- ISO 27010 (Information Technology Security Techniques): Presents strategies on methods for sharing information with trusted counterparties

- ISO 20022 (Exchange of Electronic Messages Between Financial Institutions): Defines Cross-border payment

- Cloud Data Management Capabilities (CDMC) Framework: Highlights the 14 controls for the management and protection of sensitive data in a cloud environment

b. Structural
- IFLA LRM: Conceptual entity–relationship model developed to express the logical structure of bibliographic information

- BibFrame: Foundation for the future of bibliographic description, both on the web, and in the broader networked world that is grounded in Linked Data techniques

c. Semantic
- ISO 25964 (The international standard for thesauri and interoperability with other vocabularies)

- Open Cybersecurity Schema Framework (OCSF): An extensible framework for developing schemas, along with a vendor-agnostic core security schema

d. Organisational
- Electronic Identification, Authentication and Trust Services (eIDAS): An EU regulation on electronic identification and trust services for electronic transactions

4. What are the illustrative examples of the key data management and technological controls required during data collaboration?

Below are some illustrative examples of key controls during data collaboration:

a. Data Loss Prevention (DLP) Technologies: Network DLP, endpoint DLP and cloud DLP

b. Common Encryption Methods: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Triple DES, Twofish

c. Advanced Encryption Methods: Post-quantum crypto and Quantum Key Distribution (QKD)

d. Secure Cloud Connection: HTTPS, POPS, SMPTPS, MAPS, NNTPS

e. Data Disposal Methods: Erasure, degaussing, overwriting, drive destruction

5. What are the examples of privacy preservation techniques and privacy enhancing technologies (PETs) the banks can consider?

Below are some illustrative examples:

a. Privacy Preservation Techniques: K-anonymity, randomisation, cryptographic techniques, Multidimensional Sensitivity Based Anonymisation (MDSBA)

b. Privacy Enhancing Technologies (PETs): Communication anonymisers, obfuscation, homomorphic encryption, differential privacy, pseudonymisation, federated learning

6. What are the examples of sandboxes?

Across ASEAN, there are various existing/ emerging sandboxes available:

a. Regulatory Sandboxes: GSM Association (GSMA) ASEAN cross-border data flows (CBDF) sandbox, Bank of Thailand (BOT) FinTech regulatory sandbox, Monetary Authority of Singapore (MAS) FinTech Regulatory Sandbox

b. Privacy Sandboxes: Google Privacy sandbox, Infocomm Media Development Authority (IMDA) Privacy Enhancing Technologies (PET) sandbox

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.