ASEAN Bankers Association

ASEAN Banking Interoperable Data Framework (IDF)

Safe and secured cross-border flow of data

Supporting Document

THE BRUNEI ASSOCIATION OF BANKS

THE ASSOCIATION OF BANKS IN CAMBODIA

PERBANAS
INDONESIAN BANKS ASSOCIATION

LAO BANKERS' ASSOCIATION

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

Myanmar Banks' Association

BANKERS ASSOCIATION OF THE PHILIPPINES

abs
The Association of Banks in Singapore

สมาคมธนาคารไทย

VNBA

Version 1.0 November 2022

Contents

Introduction

This Supporting Document is intended to be read in conjunction with the ASEAN Banking Interoperable Data Framework (Framework). It consolidates the ASEAN Member State regulators' survey responses to questions related to general, data sovereignty/ localisation, cross border data sharing, data management and data security requirements that readers may have while reading the Framework. It aims to support the Framework and provide more context on the Framework's Appendix which summarise the regulatory compliance considerations for ASEAN Member States.

This Supporting Document is organised in alphabetical order. All information, content, and materials available in this document are for general informational purposes only. 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.

Brunei

General

1. **What are the key regulatory requirements section data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   - Brunei Darussalam Central Bank (BDCB)'s Guidelines on Technology Risk Management (TRMG) for Financial Institutions (TRS/ G-2/ 2022/ 1) — Consumer data protection is covered in S10
   - Brunei's Personal Data Protection Order (PDPO) - The Personal Data Protection Order under the authority of AITI is still in consultation/ draft stage currently
   - Government's Data Protection Policy
   - Banking confidentiality and allowable data disclosure is contained in the Islamic Banking Order 2008/ Banking Order 2006 (THIRD SCHEDULE)

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   Authority for Info-Communications Technology Industry or AITI (as Interim Data Protection Office) and Brunei Darussalam Central Bank.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   No.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   Currently, there is no data protection legislation in Brunei Darussalam. However, the Authority for Telecommunications Technology (AITI) of Brunei Darussalam has drafted the Public Consultation Paper on Personal Data Protection for the Private Sector in Brunei Darussalam (PDPO) dated 20 May 2021.

   The draft PDPO has been developed and prepared to set out a general framework for data protection for the private sector in Brunei Darussalam. The PDPO is intended to be enacted by mid-2022. Enforcement of the PDPO will only commence 2 years from the time the PDPO is enacted.

   Under Section 4.13.1 of the Transfer Limitation Obligation of the PDPO, an organisation must not transfer personal data to a country or territory outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO.

   Therefore, our Reponses to the following questions will be based on the Public Consultation Paper on PDPO:

   a) Questions 2 under Data Sovereignty/ Localisation
   b) Questions 2 on Cross Border Data Sharing
   c) Questions 2, 3, 4, 5, 6, 7 and 8 under Cross Border Data Sharing

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

   Data disclosure must compliant with the Islamic Banking Order 2008/ Banking Order 2006 (THIRD SCHEDULE) which summarily means consent unless requested by authorities.

4. **What are the conditions to obtain the approval?**

   Authority approval for data disclosure not required unless outside of the scope of the Islamic Banking Order 2008/ Banking Order 2006.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

   Brunei Darussalam Central Bank.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Paragraph 10.1 of BDCB's Guidelines on Technology Risk Management for Financial Institutions (TRS/ G-2/ 2022/ 1).

   Insofar as Third-Party storage or outsourcing is required, this is contained in the Guidelines on Information Technology Third Party Risk Management (ITTPRMG).

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   Under Section 4.2.1 of the Transfer Limitation Obligation of the PDPO, an organisation must not transfer personal data to a country or territory outside Brunei Darussalam except in accordance with requirements prescribed under the PDPO to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPO.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   As described above.

4. **What is the process to obtain approval to share data?**

   The ITTPRMG sets out the conditions for third party storage. As this would amount to an outsourcing, adherence to the Outsourcing Guidelines 7 Sep 2012 is required and regulatory approval is required for any material outsourcing arrangements which does not state the timeframes but which we estimate to be 6 — 8 weeks.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   The estimated timeframe is 6 – 8 weeks.

6. **What are the conditions to obtaining the approval?**

   Adherence to the requirements set out in the ITTPRMG and the Outsourcing Guidelines 7 Sep 2012.

7. **Which government authorities are required to provide approvals?**

   Brunei Darussalam Central Bank.

8. **What government interventions are needed to support cross border data storage?**

   Storage of data outside of the country will require specific approval by the Brunei Darussalam Central Bank under the Outsourcing Guidelines 7 Sep 2012.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Paragraph 10.1 of BDCB's Guidelines on Technology Risk Management for Financial Institutions (TRS/ G-2/ 2022/ 1).

   Data confidentiality is also contained in S58 Islamic Banking Order 2008 and Banking Order 2006.

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   Not specifically, although the Islamic Banking Order 2008 and Banking Order 2006 (THIRD SCHEDULE) does set out what exemptions exist for the type of persons data is to be disclosed to and the purposes for the disclosure.

   Under Section 3.2.1 of the PDPO, *personal data includes data which may be of a more sensitive nature, for example, data concerning the physical or mental health of an individual, financial information, genetic data, biometric data and personal history involving any criminal offence*.

   However, the PDPO does not expressly recognise a distinction between sensitive and non-sensitive categories of personal data or define a category of sensitive personal data. It is proposed that the PDPO applies across all types of personal data as a baseline, although sector-specific frameworks may address specific concerns relating to different types of data (e.g. financial data).

3. **In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?**

   Personal data refers to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the Financial Institution (FI) has or is likely to have access.

   Under Section 3.2.1 of the PDPO, *personal data includes data which may be of a more sensitive nature, for example, data concerning the physical or mental health of an individual, financial information, genetic data, biometric data and personal history involving any criminal offence*.

4. **What are the protection requirements (system-enabled) for personally identifiable information?**

   Protection requirements (system-enabled) for personally identifiable information are set out in the Guidelines on Technology Risk Management, as follows:

   10.1.4 Any major changes to the FIs' customer-facing system, especially changes to data structure or data input field should be communicated to the customers such as in version history list or release notes.

   10.1.7 FIs should also provide clear disclaimers if their customer-facing system automatically collects data such as via cookies or data analytic tool.

10.1.9 The FIs should be able to demonstrate that the storage of customer personal data is secure and when required, to clearly indicate the controls in place to the customers.

10.1.10 When sending over customer personal information such as bank statement or payment receipt online, the FIs should arrange adequate protection such as encryption to protect the data from unauthorised receiver.

10.1.12 The FIs should ensure that customer personal data can be tracked such as using homogeneous data structure, or at least can be traced through system audit trail, database logs and file version history.

10.1.15 If the FIs must assign a third party to process customer personal data, the FIs should inform the customer on this arrangement and to limit access to personal data such by using pseudonymisation technique or encryption.

---

5. What are the protection requirements (manual controls) for personally identifiable information?

Protection requirements (manual controls) for personally identifiable information are set out in the Guidelines on Technology Risk Management, as follows:

10.1.1 When it is necessary to collect customer's personal data, the FIs should clearly indicate the purpose of the data collection and have in place a suitable method to obtain consent from the customer.

10.1.2 Data protection or privacy policy should be established or to be included in the terms and conditions and made available to the customer.

10.1.3 FIs should communicate any changes to the privacy policy or terms and conditions, and to request for renewed consent if the changes affect data protection and privacy policy.

10.1.5 When there are changes that require additional consent, negative consent method should not be used. The FIs should follow up with the customer to obtain the consent.

10.1.6 FIs should not gain consent through force or unsolicited way. Instead, the FIs may communicate the consequences or limitations on the FIs' side if the FIs are unable to obtain necessary consent to the customer's personal information.

10.1.8 FIs should ensure their customer personal data are accurate, current and complete. The FIs should establish relevant process to request or allow customers to review and update their personal data.

10.1.11 The FIs should establish relevant processes to handle customers request for information on how the FIs have been using their personal data over certain period, and in the event the customers withdraw their consent.

10.1.13 FIs should review the purpose of customer personal data and ensure the use of the personal data remains relevant to the consented purpose, especially when there are changes to the FIs systems or processes that can affect the customer's personal data.

10.1.14 If the customer personal data must be stored on a cloud platform or other third party, such arrangement including country where the customer's personal data is stored should be informed to the customer. Access to the customer personal data should be restricted

10.1.15 If the FIs must assign a third party to process customer personal data, the FIs should inform the customer on this arrangement and to limit access to personal data such by using pseudonymisation technique or encryption.

10.1.16 FIs should also be mindful of any applicable statutory or regulatory requirements on data retention, that may include retention of customer personal data. Where necessary, these requirements should be communicated to the customer.

6. **What are the restrictions on the use of PII data? How long are the restrictions for?**

   Currently there are no safeguards or restrictions placed on private sector organisations as to how they handle personal data.

7. **Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.**

   The PDPO does not state any specific requirements on assessment however the PDPO provides that an organisation is required to make an assessment where there is a data breach and to notify the responsible authority of such data breach.

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

   In written or system-enabled control, but subject to the respective banks process.

   Where consent is required, this is to be in writing. There are currently no specific guidelines requiring express written consent or prohibiting implied consent through agreement via Terms and Conditions.

   Under Section 4.6 of the PDPO, *an individual's consent is required before an organisation can collect, use or disclose such individual's personal data, unless otherwise required or authorised by law or an exception in the PDPO applies. Such consent must be validly obtained and may be either expressly given or deemed to have been given.*

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Paragraph 7.2 of BDCB's Guidelines on Technology Risk Management (TRS/ G-2/ 2022/ 1).

   In addition, guidelines in relation to management of third parties in relation to data handled in a third-party arrangement is contained in Guidelines on Information Technology Third Party Risk Management (ITTPRMG).

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   In relation to management of third party and in relation to consumer engagement within the ITTPRMG.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   Subject to the data asset management framework of the respective banks.

   In relation to management of third party and in relation to consumer engagement.

4. **Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?**

   As this is a Guideline issued by the Authority, any breaches would be subject to the general penalties under the Islamic Banking Order 2008/ Banking Order 2006.

5. **Does the policy specify which data quality dimensions to be measured?**

   No.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   No. Guidelines set out the minimum standards for collection of data only — this is set out in Section 10 of the Guidelines for Technology Risk Management. Data standards adopted by the Bank draw from requirements to adhere to the Criminal Asset Recovery Order 2012 and data required for business, operational and marketing needs.

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   Recommended and open to any international standards.

   References to any data protection laws are generally made to the following countries:

   a. Personal Data Protection Act (PDPA) in Singapore
   b. Personal Data Protection Act 2010 (PDPA) in Malaysia
   c. EU General Data Protection Regulation (GDPR) 2016/ 679

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Paragraph 7.3 of BDCB's Guidelines on Technology Risk Management (TRS/ G-2/ 2022/ 1).

   In addition, the Draft Personal Data Protection Order (PDPO) was developed in 2021.

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   Paragraph 7.2 and 8.2 of BDCB's Guidelines on Technology Risk Management (TRS/ G-2/ 2022/ 1).

3. **Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?**

   No.

Cambodia

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   - National Bank of Cambodia (NBC) — Technology Risk Management Guideline (NBC-TRMG)
   - Article 47 related to the Professional Secrecy of the Law on Banking and Financial Institutions

   Laws applicable to Banks and Financial Institutions are listed in NBC website.

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   The National Bank of Cambodia (NBC) and the Banking and Financial Institutions (BFIs).

   This is captured in Paragraph 4 of the Technology Risk Management Guidelines:

   The NBC will review the progress of implementing these guidelines. The NBC will examine the comprehensiveness and efficacy of the implementation of these guidelines and validate whether they are commensurate with the nature and scope of operations of individual BFIs from 2019.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   National Bank of Cambodia-Technology Risk Management Guideline (NBC-TRMG).

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   Laws do not explicitly restrict the storage of data outside the country. But currently we have the NBC-TRMG which allows the data storage outside the country under the cloud computing program but approval from NBC is required.

   This is captured in Section 3.6.3.b.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

   Not Applicable (N.A.). Currently we (General Directorate of Banking Supervision) have only:

   - the request on customer data sharing and the uniform template report to the parent bank (applicable for the only foreign bank and subsidiary only), and
   - seeking approval on the data sharing in cloud computing program.

4. **What are the conditions to obtain the approval?**

In the form of (1) customer data sharing and the uniform report template of the foreign branch and subsidiary only and (2) cloud computing, the specific conditions for cloud computing (captured in Section 3.6.3.b) are as follows:

---

a) Enterprises need to be particular in choosing a provider. Reputation, history and sustainability should all be factors to consider. Sustainability is of importance to ensure that services will be available, and data can be tracked;
b) Enterprises need to seek prior approval from the regulator and confirm to the regulator on the specifics of geographic location of data hosted in the cloud;
c) The cloud provider often takes responsibility for information handling, which is a critical part of the business. Contractual agreement with the cloud service provider should include penalties for failing to perform to the agreed-upon service levels impacting confidentiality, availability and integrity of data;
d) The geographical location of data storage and processing needs to be defined for the cloud data hosting. Trans-border data flows, business continuity requirements, log retention, data retention, audit trails are issues that need to be covered in the contractual agreement;
e) Third-party access to sensitive information creates a risk of compromise to confidential information. It is necessary to ensure the protection of intellectual property (IP), trade secrets and confidential customer information hosted on the cloud;
f) The contractual issues in the cloud services must include coverage related to ownership of intellectual property, unilateral contract termination, vendor lock-in, fixing liability and obligations of cloud service providers, exit clause, etc. ;
g) Due to the dynamic nature of the cloud, information may not immediately be in the event of a disaster. Business continuity and disaster recovery plans must be well documented and tested. The cloud provider must understand the role it plays in terms of backups, incident response and recovery. Recovery time objectives should be stated in the contract;
h) The incident management controls for the data hosted in the cloud should be drafted in the contractual agreement with the cloud service provider and
i) The following points should be addressed from a legal perspective:
- *Whether the user or company subscribing to the cloud computing service own the data;*
- *Whether the cloud computing system, which provides the actual storage space, own it and*
- *Whether it is possible for a cloud computing company to deny a client access to that client's data.*

---

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

The NBC is supposed to be the approval authority if in the form of (1) customer data sharing and the uniform report template of the foreign branch and subsidiary only and (2) cloud computing.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

According to NBC-TRMG in Section 4.1(iii) on Risk Management in Outsourcing Arrangements (Reporting to the Regulator).

BFIs must report to the regulator, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology/ process outsourcing and when data pertaining to Cambodian operations are stored/ processed abroad.

---

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   Currently, we have Article 47 regarding the Professional Secrecy from the law on the Law on Banking and Financial Institutions that does not allow the individual to share any confidential information related to accounting or administrative documents.

   And within the TRBG we also consider having the cloud computing but prior approval from the NBC is required (Section 3.6.3.b).

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   As mentioned above, the type of data is confidential information related to accounting or administrative documents.

4. **What is the process to obtain approval to share data?**

   Currently we (General Directorate of Banking Supervision) have only the request on customer data sharing and the uniform template report to the parent bank (applicable for the only foreign bank and subsidiary only) and for cloud computing.

   The process to obtain the approval to share data is on a case-by-case basis. We are working in the process to simplify the approval process.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

6. **What are the conditions to obtaining the approval?**

   Currently we (General Directorate of Banking Supervision) have only the request on customer data sharing and the uniform template report to the parent bank (applicable for the only foreign bank and subsidiary only) and for cloud computing.

   The conditions to obtain the approval to share data is on a case-by-case basis. We are working in the process to simplify the approval conditions.

7. **What government authorities are required to provide approvals?**

   National Bank of Cambodia.

8. **What government interventions are needed to support cross border data storage?**

   From our observation, to support the cross border data storage, the government (NBC) may need to update the TRMG and develop a clear, more precise section regarding the cross border data storage.

   For instance, the guideline should clearly address how to manage and mitigate the risks related to the cross border data storage.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   There are guidelines/ regulations related to:

a) NBC-TRMG (3.1.10 on Data Security)
b) Sub-decree: How to manage, use, and secure personal information which released by Ministry of Interior
c) Article 47 regarding the Professional Secrecy from the law on the organization and conduct of the National Bank of Cambodia that does not allow individuals to share any confidential information related to accounting or administrative documents

2. Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?

No.

3. In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?

Full name, Sex, Date of Birth, Place of Birth, Current Address, Nationality, and other information about an individual who can be identified.

4. What are the protection requirements (system-enabled) for personally identifiable information?

As highlighted in the NBC-TRMG:

- Use encryption technologies to sensitive information to encrypt data-at-rest (data storage), data-in-use (endpoint action) and data-in-transit (network action)
- Data Leak Prevention (DLP)
- Mobile Device Management (MDM)
- Access control management
- Data discovery tool to identify storage of sensitive data sets

5. What are the protection requirements (manual controls) for personally identifiable information?

As highlighted in the NBC-TRMG:

- Define data disposal procedure
- Define Data classification procedure
- Define Data protection requirement
- Perform data flow analysis to identify movement of personal data

6. What are the restrictions on the use of PII data? How long are the restrictions for?

Restriction to access based on business-need-to-do basis, in terms of system functions, privileged access, and even getting a printout of the PII.

Per TRMG Point 3.1.10,

BFIs should maintain the security of media while in transit or when shared with third parties and BFIs may encrypt customer account and transaction data sent for printing while it is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

---

7. Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.

Requirement to establish uniform risk-based requirements for the protection of data elements.

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

   There is no mention about consent obtained from data subjects.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   NBC-TRMG.

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   NBC-TRMG: Section 3.5.1 on Information security and information asset lifecycle.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   NBC-TRMG: Section 3.1.10 on Data Security.

4. **Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?**

   Not mandatory by law yet, and no penalty for non-compliance.

5. **Does the policy specify which data quality dimensions to be measured?**

   It does.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   It has.

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   - ISO/ IEC 27001-2013: Information technology — Security techniques — Information security management systems
   - Payment Card Industry Data Security Standard (PCI-DSS)

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   NBC-TRMG: Section 3.1.10 on Data Security.

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   Section 3.2.3 on Incident Management.

3. Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?

No penalties.

Indonesia

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   - Bank is required to place Electronic Systems in Data Centres and Disaster Recovery Centres in the territory of Indonesia, as per Article 21 OJK Regulation No. 38/ POJK.03/ 2016 as amended by OJK Regulation No. 13/ POJK.03/ 2020
   - Undang-Undang (UU) No. 11/ 2008: Informasi Dan Transaksi Elektronik (ITE)
   - UU No. 19/ 2016: Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
   - Peraturan Kementerian Komunikasi dan Informatika Republik Indonesia (PermenKominfo) No. 20/ 2016: Perlindungan Data Pribadi Pada Sistem Elektronik
   - Peraturan Pemerintah (PP) No. 71/ 2019: Penyelenggaraan Sistem dan Transaksi Elektronik
   - Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi (PDP)

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   - Otoritas Jasa Keuangan (OJK) / Indonesia Financial Services Authority
   - Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo)

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   According to OJK Regulation No. 38/ POJK.03/ 2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks and OJK Regulation No. 13/ POJK.03/ 2020 concerning Amendment to OJK Regulation No. 38/ POJK.03/ 2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks.

   PP No. 71/ 2019: Penyelenggaraan Sistem dan Transaksi Elektronik.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   Bank is required to placed Electronic Systems in Data Centres and Disaster Recovery Centres in the territory of Indonesia. Bank may only place Electronic Systems in Data Centres and/ or Disaster Recovery Centres outside the territory of Indonesia after obtaining approval from OJK. Electronic systems that can be placed in Data Centres and/ or Disaster Recovery Centres outside the territory of Indonesia are:

   a) Electronic System used to support integrated analysis in order to comply with regulations issued by the Bank's country of origin authorities which are global in nature, including across countries;
   b) Electronic System used for risk management in an integrated manner with the Bank's head office or parent office/ main entity office outside the territory of Indonesia;
   c) Electronic System used for the implementation of anti-money laundering and counter-terrorism financing in an integrated manner with the Bank's head office or the Bank's main office outside Indonesia;
   d) Electronic System used to provide services to customers globally, which requires integration with Electronic Systems belonging to the Bank group outside the territory of Indonesia;
   e) Electronic System used for communication management between the Bank's head office and branch offices, or between subsidiaries and parent companies; and/ or

f) Electronic System used for Bank's internal management.

These are outlined in Article 21 OJK Regulation No. 38/ POJK.03/ 2016.

3. What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?

An electronic system may require data to perform its functions. In the case when the processing of electronic system placed outside Indonesia's territory requires data stored within Indonesia's territory, data can be copied (mirroring) from the original data stored within Indonesia's territory. The original data in the core banking system, however, is still required to be stored in Indonesia. There is no estimated timeframe for obtaining such approvals.

According to POJK No. 38/ POJK.03/ 2016 pasal 24 (3), the Bank has the responsibility to request OJK approval 3 months in advance.

4. What are the conditions to obtain the approval?

OJK's approval regarding the placement of electronic systems in Data Centres and/ or Disaster Recovery Centres outside the territory of Indonesia, may be granted on the condition that the Bank:

a) Meets the requirements as referred to in Article 20 paragraph (3), (4) and (5) of POJK 38/ POJK.03/ 2016.
b) Submits the results of country risk analysis;
c) Ensures that the implementation of the Electronic System outside the territory of Indonesia does not reduce the effectiveness of the supervision of OJK as proven by a statement;
d) Ensures that confidential information regarding the Bank is only disclosed if it complies with the provisions of the laws and regulations in Indonesia as evidenced by a cooperation agreement between the Bank and the Information Technology service provider;
e) Ensures that the written agreement with the Information Technology service provider contains a choice of law clause;
f) Submits a statement letter of no objection from the supervisory authority of the Information Technology service provider outside the territory of Indonesia that OJK can conduct an examination of the Information Technology service provider;
g) Submits a statement that the Bank periodically submits the results of assessments conducted by bank offices outside the territory of Indonesia on the application of risk management to the Information Technology service provider;
h) Ensures that the benefits of the plan to place the Electronic System outside the territory of Indonesia for the Bank are greater than the burden borne by the Bank; and
i) Submits the Bank's plan to improve the ability of the Bank's human resources both related to the implementation of Information Technology as well as business transactions or products offered.

This is outlined in POJK No. 38/ POJK.03/ 2016 Pasal 21 (4).

5. What is/ are the names of the government authority(ies) that grant the approvals?

Otoritas Jasa Keuangan (OJK) / Indonesia Financial Services Authority.

Cross Border Data Sharing

1. Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.

Measures regarding cross border data sharing is highly related to the regulation of placement of electronic system. Data is an impartial part of electronic system. As every electronic system needs to be in data storage and disaster recovery centre in Indonesia, the utilisation of data for such electronic systems will follow the same rule. However, if banks meet the requirements for six exceptions of electronic system that may be placed outside the territory of Indonesia (refer to question No. 2 of Data

Sovereignty), the data pertaining such systems are allowed to be shared to overseas as long as the sharing methodology is by mirroring which means the core banking systems shall still be needed to be placed in Indonesia.

Additional policies or guidance documents are as follows:

- POJK No. 12/ POJK.01/ 2017 pasal 51: Penerapan Program Anti Pencucian Uang Dan Pencegahan Pendanaan Terorisme Di Sektor Jasa Keuangan
- RUU PDP 7

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   see above.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   Every electronic system (including the data) needs to be in data storage and disaster recovery centre in Indonesia but there are six exceptions (refer to question No. 2 of Data Sovereignty).

4. **What is the process to obtain approval to share data?**

   Approval of sharing data for six electronic systems exempted from data localization needs to be obtained from the banking supervisors.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   No.

6. **What are the conditions to obtaining the approval?**

   Refer to question No. 4 of Data Sovereignty.

7. **What government authorities are required to provide approvals?**

   Otoritas Jasa Keuangan / Indonesia Financial Services Authority.

8. **What government interventions are needed to support cross border data storage?**

   No government interventions.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   The requirement for consumer data privacy is regulated under OJK Regulation No. 38/ POJK.03/ 2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks and OJK Circular Letter No. 14/ SEOJK.07/ 2014 concerning Confidentiality and Security of Consumer Data and/ or Personal Information.

   Additional policies or guidance documents are as follows:

   - POJK No. 1/ POJK.07/ 2013: Perlindungan Konsumen Sektor Jasa Keuangan
   - PP No. 71/ 2019: Penyelenggaraan Sistem dan Transaksi Elektronik 6)

- PermenKominfo Nomor 20 Tahun 2016 (tanggal 1 Desember 2016): Perlindungan Data Pribadi dalam Sistem Elektronik 5)
- RUU PDP 7

2. Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?

According to OJK Circular Letter No. 21/ SEOJK.03/ 2017 concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks, Banks must classify information based on its sensitivities. This is outlined in Section 5.2.3.1d.

According to OJK Circular Letter No. 14/ SEOJK.07/ 2014 concerning Confidentiality and Security of Consumer Data and/ or Personal Information, Consumer Personal Data and/ or Information includes name, address, date of birth/ age, phone number, mother's maiden name (for natural person), composition of directors and commissioners including identity documents in the form of Identity Cards/ passports/ residence permits (for corporate), composition of shareholders (for corporate).

Additional policies or guidance documents are as follows:

- PP No. 71/ 2019: Penyelenggaraan Sistem dan Transaksi Elektronik
- RUU PDP

3. In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?

Refer to question No. 2 of Data Privacy.

4. What are the protection requirements (system-enabled) for personally identifiable information?

According to OJK Regulation No. 38/ POJK.03/ 2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks, Banks are required to apply the principle of controlling customer data security and Electronic Banking Service transactions on every Electronic System used by the Bank. Besides, in OJK Circular Letter No. 21/ SEOJK.03/ 2017 concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks, Banks must mitigate the general and specific risks arising from Electronic Banking Services including to:

- *take adequate steps to test the authenticity of the identity and authority of customers who make transactions through Electronic Banking Services*
- *have written policies and procedures to ensure that the Bank is able to test the authenticity of the customer's identity and authority*
- *uses various methods to test authenticity based on the Electronic Banking Services risk management assessment, sensitivity, and value of stored data*
- *using authenticity testing methods ensure proper control over authorization and access rights (privileges) to the system, Database (Database), and application of Electronic Banking Services*
- *ensure that methods and procedures are implemented to protect the integrity of data, records and information related to Electronic Banking Services transactions*
- *ensure that methods and procedures are implemented to protect the integrity of data, records and information related to Electronic Banking Services transactions*
- *implement measures to protect the confidentiality of Electronic Banking Services information. Security procedures are adjusted to the level of sensitivity of the information*
- *have standards and control over the use and protection of data if the IT service provider has access to the data*

These are outlined in Section 7.3.2 of the Circular Letter.

5. **What are the protection requirements (manual controls) for personally identifiable information?**

   Refer to question No. 4 of Data Privacy.

6. **What are the restrictions on the use of PII data? How long are the restrictions for?**

   According to OJK Regulation No. 6/ POJK.07/ 2022 regarding Customer and Public Protection in Financial Service Sector and OJK Circular Letter No. 14/ SEOJK.07/ 2014 concerning Confidentiality and Security of Consumer Data and/ or Personal Information, Banks Are prohibited in any way from providing personal data and/ or information regarding its Consumers to third parties.

   The prohibition is excluded if:
   a) Consumers provide written consent; and / or
   b) required by legislation.

   This is outlined in Section II, 2(a) and 2(b) of the OJK Circular Letter No. 14.

   Additional policies or guidance documents are as follows:

   - RUU PDP pasal 37 about data retention

7. **Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.**

   According to Article 16 OJK Regulation No. 38/ POJK.03/ 2016 as lastly amended by POJK No. 13/ POJK.03/ 2020 and OJK Circular Letter No. 21/ SEOJK.03/ 2017, banks are required to implement information security controls that are based on the risk assessment of the information owned by the banks.

   Additional policies or guidance documents are as follows:

   - RUU PDP

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

   According to the OJK Regulation POJK No. 6/ POJK.07/ 2022 regarding Customer and Public Protection in Financial Service Sector, Banks must obtain written consent of the consumers before using or giving consumers' personal data to another party.

   Consent obtained from the data subjects by written approval in the form of:
   a) The choice of agree or disagree
   b) Sign of approval in documents and/ or product and/ or service agreements

   This is outlined in Section II (4) of the Surat Edaran (SE) Otoritas Jasa Keuangan (OJK) No. 14/ SEOJK.07/ 2014: Kerahasiaan dan Keamanan Data dan/ atau Informasi Pribadi Konsumen

   Additional policies or guidance documents are as follows:

   - RUU PDP pasal 19 — written and recorded verbal agreement

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Pursuant to OJK Regulation No. 38/ POJK.03/ 2016 as lastly amended by OJK Regulation No. 13/ POJK.03/ 2020, Banks are obligated to implement principle controls of data management and security in all banks' electronic system. Banks are also obligated to ensure the effective information/ data security by implementing at least the confidentiality, integrity, and availability of information. This is outlined in Section 28(3)(5).

   Additional policies or guidance documents are as follows:

   - RUU PDP

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   No, currently the existing regulation related data management do not specifically mention the roles and responsibilities of the data function within the banks.

   Additional policies or guidance documents are as follows:

   - RUU PDP Pasal 45-46

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   No, currently the existing regulation related data management do not mention the data standards that are required for the banks.

4. **Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?**

   Non-compliance of the policy will result in administrative sanction for banks by the OJK.

5. **Does the policy specify which data quality dimensions to be measured?**

   No.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   No. Currently there is no standard on data quality enforced.

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   No.

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Consumer data security by financial service institution (including banks) is included on OJK Regulation No. 6/ POJK.07/ 2022 regarding Customer and Public Protection in Financial Service Sector (Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan), replacing POJK No. 1/ POJK.07/ 2013 regarding Financial Service Sector's Customer Protection (Perlindungan Konsumen Sektor Jasa Keuangan).

   Also, as pursuant to the OJK Circular Letter No. 21/ SEOJK.03/ 2017 concerning Implementation of Risk Management in the Use of Information Technology by Commercial Banks, banks are required to implement policy, standard, and procedure on the information security. The information security procedure, including asset management, human resources management, environment and physical security, access management, IT operational security, information security monitoring, and information security incident response management. This is outlined in Section 5.2.3.

   Additional policies or guidance documents are as follows:

   - PP No. 71/ 2019: Penyelenggaraan Sistem dan Transaksi Elektronik
   - UU No. 7/ 1992: Perbankan
   - UU No. 10/ 1998: Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan
   - UU No. 11/ 2008: Informasi Dan Transaksi Elektronik (ITE)
   - UU No. 19/ 2016: Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
   - RUU PDP

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   Not specifically regulated, but it will be regulated in Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum.

3. **Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?**

   Per OJK Regulation No. 6/ POJK.07/ 2022, on Article 45, there are various administrative sanctions for banks' failure to comply with the regulation (including data loss by FIs), which are:

   a) written warning
   b) fines
   c) prohibition as main party (controlling shareholder, BoC, or BoD), according to OJK Regulation of Reassessment of Main Party of Financial Service Institutions/ Penilaian Kembali Pihak Utama Lembaga Jasa Keuangan (currently POJK No. 14/ POJK.03/ 2021 for banking industry)
   d) business activity/ product limitation
   e) business activity/ product freezing
   f) product permit revocation
   g) business permit revocation

Laos

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   The legislation related to data protection are as follows:

   - The Law on Electronic Data Protection, which governs the collection, accessibility, use, and disclosure of electronic data, protection measures, rights, and obligations of data subject and data controller
   - The Cybercrime Law regulates rules and measures for database system, computer system data, and server system protection
   - The Penal Code sets out the punishable offences and their corresponding penalties and fines for offences related to data protection
   - The Law on Telecommunications No. 09/ NA(National Assembly) dated 21 December 2011, prohibits telecommunication service providers from disclosing State or governmental classified information and telecommunications consumers' confidential matters
   - The Law on Commercial Bank No. 56/ NA dated 7 December 2018, prohibits commercial banks from disclosing customer's data without their permission
   - The Law on Electronic Transactions No. 20/ NA dated 7 December, provides the prohibition do not disclose consumers' data, digital signatures, or electronic signature certificates
   - The Instruction on Maintaining Safety of Computer Systems No. 3623/ MPT dated 11 December 2017, clarifies specific measures for maintaining the safety of computer systems
   - The Instruction on the Implementation of the Law on Electronic Data Protection No. 2126/ MPT dated 8 August 2018, clarifies and provides details on some provisions of the law
   - The Instruction on the Implementation of the Law on Cybercrime No. 2543/ MPT dated 24 September 2018

   The Ministry of Technology and Communications (MTC) is directly responsible for issuing guidance related to electronic data protection and cybercrime.

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   a) Bank of LPDR (BOL): Department of Banking Supervision, Department of Payment Protection and Information and Technology Department
   b) National Coordination Committee for Anti Money Laundering and Countering of Financing and Terrorism
   c) Ministry of Industry and Commerce (MOIC)
   d) Ministry of Technology and Communications(MTC)

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   The transfer of private data outside of Lao PDR is subject to the express consent of data subject and compliance with the law. There is no specific form in which consent must be given under the Law on Electronic Data Protection No. 25/ NA dated 12 May, 2017and other relevant regulations.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
    a. **what type of data is disallowed?**
    b. **which country(ies) for data storage is disallowed?**

    No.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

    The delivery or transfer electronic data must be performed as follows:

    - Obtain permission from the data owner and ensure that the recipient can protect that data;
    - with the consent of the data subject and guarantee that the transferee can protect such data;
    - with the encryption of important information, such as financial, accounting, and investment data;
    - without forging the source of data sent or transferred;
    - that the transfer must be in accordance with the agreement of the transferee and transferor; and that the transfer must be stopped upon refusal by transferee.

4. **What are the conditions to obtain the approval?**

    N.A.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

    The Ministry of Technology and Communications is the supervisory authority for electronic data protection and cybercrime, but it also coordinates with the Ministry of National Defence, The Ministry of Public Security, and other concerned authorities.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

    According to Article 7, relating to International cooperation, the state opens and encourages relations and cooperation with foreign countries, regional and international communities in campaigns for the prevention and combating of cybercrime through the exchange of lessons, information, experience, the upgrade of technical knowledge and the capacity building of technical staff concerned as well as identifying and certifying data and information in accordance with international agreements and treaties, which the LPDR is party to.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

    No.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

    N.A.

4. **What is the process to obtain approval to share data?**

    N.A.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

6. **What are the conditions to obtaining the approval?**

   N.A.

7. **What government authorities are required to provide approvals?**

   The Ministry of Technology and Communications.

8. **What government interventions are needed to support cross border data storage?**

   N.A. However, in practice, it is suggested to get approval from BOL prior to do so.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   N.A.

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   The Law on Electronic Data Protection No. 25/ NA dated 12 May 2017. Article 8: Type of Electronic Data are divides electronic data into:

   - General Data: General data is defined as data which may be accessed, used, and disclosed upon correct identification of the source by the relevant controller or processer. Instruction 2126 provides a non-exhaustive list of general data which includes name, position, address, telephone number, email address, incorporation details, general statistic, and academic publications
   - Specific/ Private Data: Specific data is broadly identified as data that must not be accessed, used, and disclosed unless with the permission of relevant data subjects. The examples of private data provided under Instruction 2126 includes customer information, financial information, personal background, health information, nationality, religion, project plan, budget plan, and governmental classified information

3. **In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?**

   N.A.

4. **What are the protection requirements (system-enabled) for personally identifiable information?**

   Electronic data protection must be handled in accordance with the following principles:

   - compliance with policies, laws, strategic plans, and the national socio-economic development plan;
   - ensuring national stability, security, and social order;
   - ensuring confidentiality and safety for government, individual, legal entity, or organisation data;
   - ensuring the rights and interests of the data subject; and
   - compliance to treaties and international agreements which the LPDR is a party to.

5. **What are the protection requirements (manual controls) for personally identifiable information?**

   Specific data splits into two types, government data and personal data. Lao law does not differentiate between personal data and sensitive data.

6. **What are the restrictions on the use of PII data? How long are the restrictions for?**

   N.A.

7. **Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.**

   N.A.

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

   N.A.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Data controllers are required to comply with all policies, laws, strategic plans, and the national socio-economic development planning by:

   - ensuring that all personal data that is collected or processed is done so in accordance with the national security, stability, and social order of Laos
   - ensuring that all personal data that is collected or processed is done so in accordance with the principles of confidentiality and safety as it relates to government, individual, legal entity, or organizational data
   - ensuring that the rights and interests of data subjects are always protected
   - maintaining compliance to treaties and international agreements which the LPDR is a party to
   - creating and updating a database system, database backup system, secured system, automatic data searching system, data restoring system, among others
   - complying with all other requirements or responsibilities as set forth by other LPDR laws

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   The Ministry of Technology and Communications is the supervisory authority for electronic data protection and cybercrime, but also coordinates with Ministry of National Defence, Ministry of Public Security, and other concerned authorities.

   To protect the electronic data, the Ministry of Technology and Communications has the following main powers, duties and responsibilities:

   - review and create policies, strategic plans, laws, and regulations related to electronic protection to propose to the government for consideration;
   - amplify policies, strategic plans, and laws to work plans and projects related to electronic data protection and implement such plans;
   - supervise, manage, follow up, and inspect the services as to the laws and regulations related to electronic data protection and their implementation;
   - review, create, and use technical standards for data security;
   - manage the national electronic security code approval system;

- inspect the gaps in data system security;
- create, improve, and develop human resources in the electronic data protection field;
- consider and resolve requests related to electronic data protection;
- coordinate with other ministries concerned with electronic data protection;
- collaborate and cooperate with other countries on electronic data protection matters;
- summarise and report the electronic data protection work operations to the government regularly; and
- use other rights and perform other duties as defined by the laws.

3. Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.

According to the Law on Electronic Data Protection No. 25/ NA dated 12 May 2017.

Data controllers have the following obligations:

- secure specific data of the data subject, and for government data they must have the maintenance and administration system in accordance with the level of data security as specified in the Law;
- accessing, using, disclosing, providing, updating, terminating, editing, or deleting the electronic data on the request of data subject;
- responsibility for data that has been damaged;
- provide information to relevant officers for finding offenders;
- administer the maintenance system and equipment for storing electronic data;
- ensure the access, use, disclosure, sending, and transfer of electronic data without effecting the stability of the nation and the orderliness of society;
- create and update the database system, database backup system, secured system, automatic data searching system and data restoring system, among others;
- coordinate with the post and telecommunication sectors regarding security from data attacks;
- ensure measures on the resolution of technical problems;
- research and use information technologies to meet the social demands; and
- comply with other obligations as specified in LPDR law.

4. Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?

N.A.

5. Does the policy specify which data quality dimensions to be measured?

N.A.

6. Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?

N.A.

7. In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?

N.A.

Data Security

1. Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.

In terms of sanctions with respect to non-compliance, the Law on Electronic Data Protection No. 25/ NA dated 12 May 2017 is enforced through the Penal Code No. 26/ NA dated 17 May 2017, or the Penal

Code for short. As such, penalties that can be imposed against data controllers in Laos who fail to comply with the law include:

- Warnings and re-education
- Disciplinary action in instances where government officials violate the law
- Fines of LAK 15 million in case of engagement in a prohibited action which does not constitute a criminal offense
- The application of criminal sanctions based on the seriousness of the wrongful act

2. Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website

N.A.

3. Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?

N.A.

Malaysia

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   - Personal Data Protection Act 2010 (PDPA) — Applicable to any person who processes and has control over or authorises the processing of any personal data in respect of commercial transactions (i.e., data user)
   - Personal Data Protection Standard 2015
   - Personal Data Protection Code of Practice for the Banking and Financial Sector (PDPCOP)
   - Financial Services Act 2013 (FSA) and Islamic Financial Services Act 2013 (IFSA) (Information and secrecy provisions) — Applicable to financial institutions
   - Policy document on Management of Customers Information and Permitted Disclosures (MCIPD) — Applicable to financial institutions
   - Policy document on Risk Management in Technology (RMiT) — Applicable to financial institutions
   - Central Bank of Malaysia Act 2009 — Applicable to the Central Bank of Malaysia

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   PDPA 2010, Personal Data Protection Standard 2015, and PDPCOP — Personal Data Protection Commissioner and Ministry of Communications and Multimedia Malaysia.

   All other items — Bank Negara Malaysia (BNM).

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   None by BNM, subject to prudential grounds and certain approval processes if necessary.

   However, the PDPA technically prohibits the transfer of personal data outside of Malaysia unless the transfer is to a country with sufficient data protection laws, as specified by the Minister in a Government Gazette, which will be based on the Personal Data Protection Commissioner's recommendation to the Minister (of Communications and Multimedia). Notwithstanding the prohibition, the PDPA expressly permits the transfer of personal data abroad under certain conditions, for example, if it was consented to by the data subject, or if in furtherance of the contract with the data subject etc. This is outlined in Section 129 of the Act.

   The above is also echoed in the Outsourcing Policy Document published by BNM where it states that if any data is transferred out of Malaysia, the service provider is subject to data protection standards that are comparable to Malaysia.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   No.

3. What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?

There are no processes specifically required to obtain approval to share copies of data, although there are general requirements relating to use, disclosure and transfer of personal data under the PDPA (see #Q1 above).

Under MCIPD, the disclosure of customer information is permitted under Schedule 11 of FSA / IFSA and Paragraph 13.2 of MCIPD. Otherwise, BNM's approval is required.

However, financial institutions are required to consult BNM and conduct Risk Assessment for the use of public cloud for critical systems. This is not an approval requirement. The consultation session with BNM is to demonstrate that financial institutions have thoroughly considered and addressed the risks outlined in Paragraphs 10.49 and 10.51 of the RMiT. A formal notification letter is expected to be submitted to BNM after the consultation session.

4. What are the conditions to obtain the approval?

Under MCIPD, financial institutions intending to apply for BNM's approval for disclosure of customer information under Section 134(1)(b) of the FSA (or Section 146(1)(b) of the IFSA) must complete and submit the application form in Appendix V of the Guidelines on Management of Customer Information and Permitted Disclosure to BNM.

Under RMiT, where a financial institution is required to consult BNM and conduct risk assessment for the use of public cloud for critical systems (Note: As per #Q3 above, this is not an approval requirement):

---

1) The financial institution is expected to demonstrate that specific risks associated with the use of cloud services for critical systems have been adequately considered and addressed. Adequate risk assessment, which shall (among others) address the following areas:

a) the adequacy of the over-arching cloud adoption strategy of the financial institution including:

i. board oversight over cloud strategy and cloud operational management;
ii. senior management roles and responsibilities on cloud management;
iii. conduct of day-to-day operational management functions;
iv. management and oversight by the financial institution of cloud service providers;
v. quality of risk management and internal control functions; and
vi. strength of in-house competency and experience.

b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas:

i. information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and
ii. cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit.

c) the degree to which the selected cloud configuration adequately addresses the following attributes:

i. geographical redundancy;
ii. high availability;
iii. scalability;
iv. portability;
v. interoperability; and
vi. strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.

2) If needed, the financial institution should consider having a third-party review that covers among others, the items in (1) above

---

It should be noted that the RMiT used the word *Consultation* denoting a two-way communication as opposed to an outright approval application.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

   For MCIPD, approval from BNM is required.

   For RMiT, no approval from BNM is required.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   There are no specific guidelines issued by BNM on cross border data sharing.

   However, the MCIPD and RMiT do have provisions on data sharing. Also, the PDPA and PDPCOP would be applicable.

   The relevant sections have been listed above.

   In addition, under BNM's Blueprint (Financial Sector Blueprint 2022-2026), BNM will be supporting regional data sharing initiatives.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   Given the question, we view that the response can cover the relevant acts that is applicable to all sectors including the financial institutions as well as BNM.

   a) Personal Data Protection Act (PDPA) — Applicable to any person who processes and has control over or authorises the processing of, any personal data in respect of commercial transactions (i.e. data user).

      For non -banking sector- Section 129(1) of the PDPA currently prohibits the transfer of any personal data outside of Malaysia, unless the recipient countries have been whitelisted by the Communications and Multimedia Minister (Minister) in the Federal Gazette. However, there are exceptions to this restriction, including the following:

      a) The data subject has given his or her consent to the transfer
      b) The transfer is necessary for the performance of a contract between the data subject and the data user
      c) The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner that would contravene the PDPA
      d) The transfer is necessary to protect the data subject's vital interests
      e) The transfer is necessary as being in the public interest in circumstances as determined by the Minister

      Nevertheless, the Ministry-in-charge is considering amendments to the PDPA i.e. replacing the white-list regime under Section 129 of the PDPA with a black-list regime. Under the black-listing regime, data users will generally be allowed to transfer personal data overseas, save and except for jurisdictions which have been black-listed by the Minister.

   b) Central Bank of Malaysia Act (CBA) — Applicable to the Central Bank of Malaysia

      78(6) The Bank may publish in any manner it deems fit, consolidated statements of all or any part of the record of international accounts, aggregating the data, information or particulars in

documents received or obtained under Subsection (2), provided that such publication shall not in any manner lead to the identification of any person to which such data, information, or particulars relate.

47(d) such other person as the Bank thinks fit, in order to compile information or data or conduct research for the purpose of giving effect to the objects and carrying out the functions of the Bank under this Act, provided that any publication by the Bank or such other person of the information, data or research shall be consolidated or aggregated and shall not in any manner lead to the identification of any customer of a financial institution to which such information, data or research relate

---

3. If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?

Any personal data pertaining to a data subject in Malaysia. For information, personal data means any information in respect of commercial transactions which:

---

a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
c) is recorded as part of a filing system or with the intention that it should form part of a relevant filing system.

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession or a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

This can be found in Section 4 of the PDPA.

CBA Specific — Individual and transactional data that lead to specific disclosure of entity

4. What is the process to obtain approval to share data?

- PDPA

  Requests to share data outside of Malaysia would require approval from the Minister unless falling under the exceptions as stated in the response for Q2 of this section. In future, this regime could be changed where approval is not required for data flowing outside of Malaysia and prohibition only applicable to sharing of data outside Malaysia to black-listed countries (i.e. approach is under review).

- MCIPD

  The disclosure of customer information is permitted under Schedule 11 of FSA / IFSA and Paragraph 13.2 of MCIPD. Otherwise, Bank Negara Malaysia's approval is required.

5. Is there an estimated timeframe to which such approvals are obtained?

N.A.

6. What are the conditions to obtaining the approval?

Under MCIPD, financial institutions intending to apply for BNM's approval for disclosure of customer information under Section 134(1)(b) of the FSA (or Section 146(1)(b) of the IFSA) must complete and submit the application form in Appendix V of the Guidelines on Management of Customer Information and Permitted Disclosure to BNM.

7. What government authorities are required to provide approvals?

Personal Data Protection Commissioner under the Ministry of Communications and Multimedia Commission (MCMC), who then shall make recommendations to the Minister.

For MCIPD, approval from BNM is required.

For RMiT, no approval from BNM is required.

8. What government interventions are needed to support cross border data storage?

Amendments to the PDPA would be required which is currently on-going.

Personal Data Privacy

1. Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.

- Financial Services Act (FSA) 2013 and Islamic Financial Services Act (IFSA) 2013 — Applicable to financial institutions.

  The banking industry is required to adhere to secrecy provisions specified under Section 133 of the Financial Services Act (FSA) 2013 and Section 145 of the Islamic Financial Services Act (IFSA) 2013. Under these provisions, any person with access to documents or information relating to the affairs or accounts of any customer of the bank are prohibited from disclosing the documents or information to another person.

- PDPCOP and Personal Data Protection Standard 2015

2. Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?

Section 4 of the PDPA defines sensitive personal data as any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette.

Section 6(1) of the PDPA prohibits data users from processing sensitive personal data about a data subject unless explicit consent was given or the processing is necessary for the purpose of exercising or performing any right or obligation required by law or to protect the vital interests of the data subject or another person.

3. In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?

Section 4 of the PDPA defines personal data as any information in respect of commercial transactions which:

a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
c) is recorded as part of a filing system or with the intention that it should form part of a relevant filing system;

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Management of Customers Information and Permitted Disclosures (MCIPD) — Applicable to banking institutions

Paragraph 5.1 of BNM's policy document on MCIPD defines customer information as any information relating to the affairs or, in particular, the account, of any particular customer of the financial service provider in whatever form including in the form of a record, book, register, correspondence, other document or material.

4. What are the protection requirements (system-enabled) for personally identifiable information?

Section 9(1) of the PDPA requires that when processing personal data, the data user to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to, among others, any security measures incorporated into any equipment in which the personal data is stored.

There are other related policy documents(PD) and exposure draft(ED) on protection requirements:

a) PD on MCIPD (relevant paragraphs — 10.12 and 10.13) – system-enabled only
b) PD on RMiT – covers both system-enabled and manual controls
c) PD on Interoperable Credit Transfer Framework (relevant paragraphs – 11.1 and 11.2) -covers both system -enabled and manual controls & Q6 below
d) ED on E-money (relevant paras 18.14, 28.2, 28.5, among others) – covers for both system-enabled and manual controls & Q6 below
e) ED on Payment System Operator (PSO) (relevant paras — 17.2 and 17.3) -covers for both system-enabled and manual controls &Q6 below

Additional documents include PDPA Section 9(2), PDPCOP Section 3.4.5 and 3.4.6, Personal Data Protection Standard 2015 Section 4.1

5. What are the protection requirements (manual controls) for personally identifiable information?

- PDPA – specific to manual controls
  Section 9(1) of the PDPA requires that when processing personal data, the data user to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to, among others:

a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;
b) the place where the personal data is stored;
c) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
d) the measures taken to ensure the secure transfer of the personal data.

- MCIPD – specific to manual controls
  Paragraph 10.6 of BNM's policy document on MCIPD requires banks to establish and have in place written policies and procedures to safeguard customer information, which covers collection, storage, use, transmission, sharing, disclosure and disposal of customer information.

- Policy document on RMiT includes relevant provision on this area as well
- Additional documents include PDPA Section 9(2),and Personal Data Protection Standard 2015 Section 5.1

6. What are the restrictions on the use of PII data? How long are the restrictions for?

Section 10 of the PDPA requires personal data processed for any purpose not to be kept longer than is necessary for the fulfilment of that purpose. Relevant steps are required to be taken to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was processed.

In addition, Section 6(1) states:

A data user shall not
a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or
b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of Section 40.

S.6(3) states:

Personal data shall not be processed unless
a) the personal data is processed for a lawful purpose directly related to an activity of the data user;
b) the processing of the personal data is necessary for or directly related to that purpose; and
c) the personal data is adequate but not excessive in relation to that purpose.

The restrictions apply if the data user is subject to the provisions of the PDPA, unless the processing is subject to an exception under the said Act

Paragraph 10.32 of BNM's policy document on MCIPD requires banks to have proper procedures in place to identify customer information that is no longer required from the perspective of operation or requirements of any written law. Banks are required to deploy appropriate methods to securely dispose of such customer information which includes any paper and digital records of the customer information.

7. Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.

Paragraphs 10.1 and 10.2 of BNM's policy document on MCIPD requires banks to identify potential threats and vulnerabilities that could result in theft, loss, misuse, or unauthorised access, modification or disclosure of customer information by whatever means. The assessment must include the likelihood that such threat and vulnerability will materialise and the potential impact it will have on the bank and its customers in the event a customer information breach occurs.

8. Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?

Section 7 of the PDPA specifies that a written notice must be sent to inform the data subject, among others that-

(a) the personal data is being processed by or on behalf of the data user, and to provide a description of the personal data;
(b) the purposes for which the personal data is being or is to be collected and further processed.

This notice is to be given when the data subject is first asked by the data user to provide his personal data, when the data user first collects the personal data of the data subject, in any other case, before the data user uses the personal data or discloses the personal data to a third party.

Consent must be obtained in a form that such consent can be recorded and maintained properly by the data user.

Examples of forms of consent that are acceptable are: (i) signatures or ticks indicating consent; (ii) opt-in consent; (iii) deemed consent; or (iv) verbal consent, subject to fulfilment of the requirements of the Personal Data Protection Regulations 2013 as to consent being capable of being recorded and maintained.

Aside from the above, both the FSA and IFSA also require written consent to be obtained by the customer, the executor or administrator of the customer, or in the case of a customer who is incapacitated, any other legal personal representative prior to customer documents or information is disclosed.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   - Guideline on Data Management and MIS Framework issued to Financial Institution in 2013.
   - Selected Policy Documents on data requirements (restricted access):

     a) Central Credit Reference Information System (CCRIS) Requirement on the submission, Usage and Protection of Credit Information
     b) STATsmart Reporting Requirements on Data Submission for Reporting Entities
     c) External Sector Statistics (ESS) System Submission of International Transactions and External Position Information
     d) FISS Submission of Financial Institutions Statistical Reports for Reporting Entities
     e) Reporting Requirements on Financial Inclusion Survey Submission for Reporting Entities
     f) Guidance Notes for Insurance Companies Statistical System (ICSS)
     g) Reporting Requirements for Islamic Banking Portfolio Exposure (Investment, Deposit, Derivatives and Sukuk Holding) according to Product and Shariah Approved Contracts

   - Data Quality Framework for Statistical Reporting to Bank Negara Malaysia (for data submissions) (restricted access).

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   In Principle 2 (Paragraph 4.8) of the Guidelines on Data Management and MIS Framework.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   - In the reporting requirement section in the policy documents (restricted policy documents 1-7 as shared in question 1) specify standards for data submission to BNM.

- In the Data Quality Framework for Statistical Reporting to Bank Negara Malaysia (restricted access) which establishes data quality standards for data submissions.

- The Personal Data Protection Standard 2015 prescribes the minimum requirements issued by the Personal Data Protection Commissioner in relation to the security standard, retention standard and data integrity standard

4. Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?

The policy and guide are enforceable by law, under Section 48 of the Financial Services Act 2013 (FSA) and Section 58 of the Islamic Financial Services Act 2013 (IFSA). The penalties for non-compliance are governed by Statistical Reporting Enforcement Framework (SREF) which was established under FSA Section 234 and IFSA Section 245 with administrative monetary penalty not exceeding RM5million for a breach or any other administrative actions for non-compliance of statistical reporting to BNM.

Section 5 (2) of the PDPA states that all processing of Personal Data shall be done according to the 7 personal data protection principles, failing which, a data user who contravenes Subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

In furtherance to the above, Section 143 (3) of the PDPA states that the regulations made under this Section or any other subsidiary legislation made under the PDPA may prescribe for any act or omission in contravention of the regulations or other subsidiary legislation to be an offence and may prescribe for penalties of a fine not exceeding two hundred and fifty thousand ringgit or imprisonment for a term not exceeding two years or to both.

5. Does the policy specify which data quality dimensions to be measured?

Guidelines on Data Management and MIS Framework also stated data quality in term of accuracy, completeness, consistency and currency.

PDPOC states

3.6.1 The Act provides that a Data User is to take reasonable steps to ensure that the personal data processed by the Data User is accurate, complete, not misleading and kept up-to-date, in relation to the purpose as well as the directly related purpose.

3.6.2 By way of illustration, the Act requires a Data User to take reasonable steps in order to ensure that the personal data processed in relation to a Data Subject is:

i) accurate/ correct (meaning that the personal data is captured without any inaccuracies, such as erroneously recording the Data Subject's agreement to receive direct marketing materials for other products of the Data User);

ii) complete (meaning that information in relation to the Data Subject has not been omitted, which for example may lead the Data User to make unfavourable decision in relation to a Data Subject's application for a credit card);

iii) not misleading (meaning that the personal data processed by the Data User should not — through error, omission, oversight, etc. – result in an inaccurate or false reflection of the status of the Data Subject); and

iv) kept up to date (meaning that the personal data of the Data Subject should reflect the latest verified information in respect of the Data Subject, for example a change of address or capturing a loan/ financing instalment payment made by the Data Subject).

Please refer to Section 3.6.3 for what amounts to reasonable steps, as it will differ from case to case.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   Policy documents a) to g) as stated in question 1 (restricted access) spells out minimum standards in terms of accuracy, completion, amendment of data, late submission and non-submission define in policy documents on data requirements.

   The Data Quality Framework (restricted access) for Statistical Reporting to Bank Negara Malaysia defines data quality checking rules for submitted data, including percentage/ threshold and validation rules.

   The Personal Data Protection Commissioner has prescribed some measures in relation to data integrity:

   a) Provide personal data update form for data subjects, either via online or conventional
   b) Update personal data immediately once data correction notice is received from data subject
   c) Ensure that all relevant legislation is fulfilled in determining the type of documents required to support the validity of the data subject's personal data
   d) Notify on personal data updates either through the portal or notice at premises or by other appropriate methods

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   This is not applicable to BNM, but we wish to share examples of international standard issued by international agencies on data governance such as United Nations National Quality Assurance Frameworks (UN NQAF) Manual for Official Statistics, IMF Data Quality Assessment Framework, OECD Data Governance.

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Policy document on Risk Management in Technology.

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   This is captured in Section 11 of the policy document on Risk Management in Technology.

3. **Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?**

   Severity depends on the circumstances of each case.

   Under Section 234(3) of the FSA (or Section 245(3) of the IFSA) subject to Subsection (4), BNM may impose a monetary penalty

   a) in accordance with the order published in the Gazette made under Section 236 or if no such order has been made, such amount as the Bank considers appropriate, but in any event not exceeding five million ringgit in the case of a breach that is committed by a body corporate or unincorporate or one million ringgit in the case of a breach that is committed by any individual, as the case may be;
   b) which shall not exceed three times the gross amount of pecuniary gain made, or loss avoided by such person as a result of the breach; or
   c) which shall not exceed three times the amount of money, which is the subject matter of the breach,

whichever is greater for each breach or failure to comply.

Myanmar

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   Only instructions issued by Central Bank of Myanmar (CBM).

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   Central Bank of Myanmar (CBM), Information and Cyber Security Department.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Not yet.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   Cyber Security Law issued just recently. It is not implemented yet.

   Data Sovereignty or the storage of data outside the country is not clearly stated yet.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

4. **What are the conditions to obtain the approval?**

   N.A.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

   Central Bank of Myanmar.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Cross-border Data Sharing policies are not issued yet.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   N.A.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   N.A.

4. **What is the process to obtain approval to share data?**

   N.A.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

6. **What are the conditions to obtaining the approval?**

   N.A.

7. **What government authorities are required to provide approvals?**

   Central Bank of Myanmar.

8. **What government interventions are needed to support cross border data storage?**

   N.A.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Data Privacy policies are not issued yet.

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   There are no such levels since national standards are not ready.

3. **In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?**

   No constitution yet.

4. **What are the protection requirements (system-enabled) for personally identifiable information?**

   N.A.

5. **What are the protection requirements (manual controls) for personally identifiable information?**

   N.A.

6. **What are the restrictions on the use of PII data? How long are the restrictions for?**

   N.A.

7. **Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.**

   N.A.

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

   Consents are obtained from customers for KYC and due diligence only. Not for the use of personal data.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Only high-level instructions are issued by CBM for banking data measures.

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   N.A.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   N.A.

4. **Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?**

   N.A.

5. **Does the policy specify which data quality dimensions to be measured?**

   N.A.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   N.A.

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   We followed and complied with PCI-DSS.

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   N.A.

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   N.A.

3. **Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?**

   N.A.

Philippines

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   The financial sector in the country is regulated by entities such as the Bangko Sentral ng Pilipinas (BSP) and its attached agency[1], the Philippine Deposit Insurance Corporation (PDIC).

   BSP's key mandates, functions, and responsibilities focus on three key pillars:

   a) Price / monetary stability;
   b) Financial stability; and
   c) Payments and settlement systems oversight

   In carrying out these core mandates, the BSP shall endeavour to promote financial inclusion.

   Besides, BSP's functions and responsibilities include serving as the:

   a) Sole / exclusive issuer of Philippine currency;
   b) Lender of last resort; and
   c) Banker and financial advisor of the Government

   The primary source of regulations governing banking institutions supervised by BSP is the Manual of Regulations for Banks (MORB). It provides the rules and policy issuances that implement the broader provisions of Republic Act No. 8791, also known as the General Banking Law of 2000, as well as other pertinent banking laws.

   In the case of BSP-supervised Non-Bank Financial Institutions (NBFIs), the rules and regulations set forth in the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) shall apply.

   Additionally, other pertinent regulations involving foreign exchange and other related transactions of BSP-supervised financial institutions (BSFIs), entities and individuals are covered by the Manual of Regulations on Foreign Exchange Transactions (MORFXT).

   Other statutes such as R.A. No. 1405 or the Bank Secrecy Act, R.A. No. 10173 or the Data Privacy Act (DPA), and R.A. No. 11765 or the Financial Products and Services Consumer Protection Act, among others, may also need to be considered.

   The abovementioned banking laws and BSP regulations can be found in the BSP website.

   Other regulatory requirements which should be considered are the issuances and circulars on data sharing of the National Privacy Commission (NPC).

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   Bangko Sentral ng Pilipinas (BSP), National Privacy Commission (NPC), both of which have been described in Question 1, as well as the Department of Information and Communications Technology (DICT), whose mandate is to *ensure and protect the rights and welfare of consumers and business users*

[1] By virtue of R.A. No. 11840 or the amended PDIC Charter dated 17 June 2022.

to privacy, security and confidentiality in matters relating to ICT, in coordination with agencies concerned, the private sector and relevant international bodies pursuant to R.A. No. 10844.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   This is also found in the IRR of the DPA Rule II.

   In addition, banking institutions are expected to strictly adhere to the provisions of R.A. No. 1405 or the Bank Secrecy Act and R.A. No. 6426 or the Foreign Currency Deposit Act, which likewise enforces the deposit secrecy of the former.

   Deposit information is strictly prohibited to be disclosed, examined, or inquired upon unless written permission of the depositor has been secured or in certain cases provided in Section 2 of the Bank Secrecy Act.

   Section 112 of the Manual of Regulations for Banks (MORB) on Management Contracts and Outsourcing, as amended by Circular No. 1137 dated 18 February 2022, provides guidelines on the rules on offshore outsourcing.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   No, there is no specific regulation that expressly prohibits such storage of data. The National Privacy Commission only states that

   In situations wherein the cross border transfer of personal data is necessary for processing purposes, keep in mind Section 21 of the DPA, to wit:

   Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross border arrangement and cooperation.(underscoring supplied)

   As can be gleaned from the foregoing provision, the Personal Information Controller (PIC) has the primary responsibility of securing the personal data under its control or custody, even when these are transferred across borders or jurisdictions. It shall ensure that said data are processed in accordance with the provisions of the DPA, its IRR, and other applicable issuances of the NPC. Any outsourcing, subcontracting, or data sharing agreement that facilitates such cross border transfer shall also be subject to the requirements of the law.

   In addition, with reference to Question 2, Section 112 of the Manual of Regulations for Banks (MORB) on Management Contracts and Outsourcing, as amended by Circular No. 1137 dated 18 February 2022, permits outsourcing of bank's domestic operations only when:

   1. the service agreement defines counterparties' right and responsibilities on confidentiality and data privacy, and
   2. the service provider operates in jurisdictions with existing confidentiality and/ or data privacy laws that are not in conflict with existing Philippine laws and relevant regulations.

When the service provider is in other countries, the bank should consider and closely monitor, on a continuing basis, government policies and other conditions in countries where the service provider is based during risk assessment process. The bank shall also develop appropriate contingency and exit strategies.

If reasonable means to conduct offsite procedures have been exhausted, the Bangko Sentral shall be given access to the service provider and those relating to the outsourced domestic operations of the bank. Such access may be fulfilled by on-site examination through coordination with host authorities, if necessary. The domestic subsidiary of a foreign bank shall be principally liable in cases where the clients are prejudiced due to errors, omissions and frauds of the service provider located offshore.

The Bangko Sentral may require the bank to terminate, modify, make alternative outsourcing arrangement or re-integrate the outsourced activity into the bank, as may be necessary, if confidentiality of customer information, effective customer redress mechanisms or the ability of the Bangko Sentral to carry out its supervision functions cannot be assured.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

4. **What are the conditions to obtain the approval?**

   N.A.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

   N.A.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Please refer to Section 50 of the IRR of the DPA.

   Philippines is also participating in the APEC Cross-Border Privacy Rules (CBPR) System.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   There are no specific prohibitions on cross border transfer of data, however, any data transfer can only take place only if minimum standards set forth by the related laws and regulations are adhered to.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   There is no specific regulation in the New Central Bank Act or the BSP Manual of Regulation for Banks that requires approval for cross border data sharing provide that the relevant consent or waiver is obtained as may be required (e.g., data includes sensitive personal information covered under the Data Privacy Law or data about the bank deposits which are covered under the Philippine laws on secrecy of bank deposits. In such a case, for personal data of bank clients, the bank shall obtain prior written consent of the client for example).

4. **What is the process to obtain approval to share data?**

   N.A.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

6. **What are the conditions to obtaining the approval?**

   N.A.

7. **What government authorities are required to provide approvals?**

   N.A.

8. **What government interventions are needed to support cross border data storage?**

   This is part of the data security measures stated in DPA of 2012.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   The Philippines has a law for data privacy enacted in 2012. This is the Republic Act No. 10173 also known as the Data Privacy Act of 2012 (DPA).

   In addition to the provisions of Republic Act No. 10173, BSFIs are required to comply with the following laws and regulations on data privacy, among others:

   - Section 8 (e) of Privacy and Protection of Client Data under Republic Act No. 11765, otherwise known as the Financial Products and Services Consumer Protection Act;
   - Section 1002 of Policies and Procedures, Consumer Protection Standards of Conduct and Appendix 78 of Information Technology Risk Management Standards and Guidelines under the MORB;
   - Circular No. 1122 on Open Finance Framework, requiring the Open Finance Oversight Committee to adopt standards, agreements, policies and guidelines (conventions) which shall at the minimum cover protection of client information including responsible date handling as well as implement the provision on data privacy and protection concerning open finance framework, and
   - Deposits and investments in bonds issued by the Government of the Philippines are classified by the Law on Secrecy of Bank Deposits (R.A. No. 1405) as of an absolute confidential nature except (1) upon written permission of the depositor, or (2) in cases of impeachment, or (3) upon order of a competent court in cases of bribery or dereliction of duty of public officials, or (4) in cases where the money deposited or invested is the subject matter of the litigation.. Foreign currency deposits are also accorded absolute confidentiality under the Foreign Currency Deposit Act (R.A. No. 6426), except upon the written permission of the depositor.

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   This is defined in the DPA, although, in the law personal data are categorized into three (3) which is used as the level of sensitivity as well. Personal data are categorized as:

   a) Personal Information (Section 3 Subsection g)
   b) Sensitive Personal Information (Section 3 Subsection l)
   c) Privilege Information (Section 3 Subsection k)

3. **In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?**

   As defined in the Chapter 1 Sec. 3(g): Personal Information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information, or when put together with other information would directly and certainly identify an individual. Further, Rule 1 Sec. 3(j) or the Implementing Rules and Regulations, Personal data refers to all types of personal information.

4. **What are the protection requirements (system-enabled) for personally identifiable information?**

   This is defined in the IRR of the DPA Rule VI. Security Measures for the Protection of Personal Data.

5. **What are the protection requirements (manual controls) for personally identifiable information?**

   This is defined in the IRR of the DPA Rule VI, Security Measures for the Protection of Personal Data.

   This is also outlined in Rule VI, Section 27 on Physical Security Measures.

6. **What are the restrictions on the use of PII data? How long are the restrictions for?**

   Use of Personal Data should be adhered to in the data principles stated in Rule IV of the IRR.

   This is outlined in Section 18 on Principles of Transparency,

   > Legitimate Purpose and Proportionality: The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

   For more details on these principles, please refer to the remainder of Rule IV of the IRR.

7. **Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.**

   DPIA or in the Philippine context, Privacy Impact Assessment. This is one of the five pillars of compliance of the National Privacy Commission.

   According to the section on Key Considerations:

   > In general, a PIA should be undertaken for every processing system of a PIC (Personal Information Controller) or PIP (Personal Information Processor) that involves personal data.

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

   This is defined in the Chapter 3 of DPA and further elaborated in the IRR Rule 4 Sec 19.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Section 171 on Reporting Governance Framework of the MORB states that *An effective governance process over the bank's reporting system must be established by the Board and implemented by senior management to ensure the bank's adherence to the reporting standards. The bank's reporting system should be supported by a combination of systems, policies and procedures that are intended to facilitate the accurate and timely generation of bank reports. A bank's periodic review of the governance process is likewise integral in determining whether the reporting system continues to be relevant and effective.*

   The BSP also has existing provisions on governance standards relating to the protection and privacy of consumer data, as provided in Circular No. 982 and No. 1048 on Enhanced Guidelines on Information Security Management and Consumer Protection Framework, respectively.

   In addition, regulations relating to open banking/ finance standards and data ownership related to technology outsourcing are provided in Circulars Nos. 1122 and 1137[2].

   Furthermore, the BSP is in the process of defining the Digital Governance Standards (the third pillar of the BSP Digital Payments Transformation Roadmap), which will ensure that the expansion of use cases is bound by sound standards that safeguard the integrity and privacy of consumer data.

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   In general, Section 3 of the Data Protection Act (DPA) of 2012 under R.A. No. 10173 applies to the banking industry, which provide the following data roles:

   (h) Personal information controller refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:
   (1) A person or organization who performs such functions as instructed by another person or organization; and
   (2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.
   (i) Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

   Relevant BSP policy is covered in Sections 2.4 on Responsibility and Accountability and 2.6 on Compliance with Relevant Laws, Regulations and Standards under Appendix A of Circular No. 982. In designing the Information Security Strategic Plan (ISSP) and Information Security Program (ISP), compliance with relevant laws, regulations, and standards must also be fully considered.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   Section 172 of the MORB provides that:

[2] Other applicable circulars: Circular No. 982, Circular No. 1048

Banks shall have a true and accurate account, record or statement of their daily transactions. For this purpose, the definition of records under Sec. 001 shall apply. The making of any false entry or the wilful omission of entries relevant to any transaction is a ground for the imposition of administrative sanctions under Section 37 of R.A. No. 7653 and the disqualification from office of any director or officer responsible therefor under Section 9-A of R.A. No. 337, as amended.

This is without prejudice to their criminal liability under Sections 35 and 36 of R.A. No. 7653 and/ or the applicable provisions of the Revised Penal Code.

The DPA provides general data privacy principles (Sec 11) that are required to be adhered to for protection of personal information. In particular, personal information must in part be: *(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted; (d) Adequate and not excessive in relation to the purposes for which they are collected and processed; (e) Retained only for as long as necessary for the fulfilment of the purposes for which the data was obtained or for the establishment, exercise or defence of legal claims, or for legitimate business purposes, or as provided by law.*

Meanwhile, BSP Circular No. 982 indicates that BSFIs may refer to leading standards and frameworks issued by standard-setting bodies on information security and cybersecurity in designing their information security risk management (ISRM).

The BSP is also in the process of developing a holistic policy on data governance and ethical use of data, which will be geared toward ensuring that all data and information obtained and passing through different digital channels will be handled ethically and that all participants will be bound by key data governance principles.

4. Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?

Please refer to the following:

Sanctions on reports for non-compliance with the reporting standards.

Definitions can be found in Manual of Regulations for Banks – Part One Page 187

1) Erroneous report – A report submitted within the prescribed deadline but is found to be non-compliant with the Bangko Sentral reporting standards described under this Section shall be classified as Erroneous.

Submission of an Erroneous Report shall be considered as wilful failure to comply with a regulation.

2) Delayed report – A report that was able to comply with the Bangko Sentral reporting standards after the submission deadline for said report shall be classified as Delayed. Submission of a compliant report after the submission deadline shall be considered as wilful delay in submission of reports.

3) Unsubmitted – A report that was not submitted, or was submitted but not able to comply with the Bangko Sentral reporting standards, by the time the next report becomes due or upon the lapse of thirty (30) banking days from the report's submission deadline, whichever comes first shall be classified as Unsubmitted. See Table 2 as reference for the defined number of banking days after

submission deadline for a report to be considered Unsubmitted. Non-submission of reports under this item shall be considered as wilful refusal to comply with a regulation[3]

For non-compliance penalties, please refer to Sanctions on reports for non-compliance with reporting standards (refer to Page 186).

In addition, Chapter VIII of the DPA provides details on various penalties. Please refer to the following sections for details:

- Section 25 Unauthorized Processing of Personal Information and Sensitive Personal Information
- Section 26 Accessing Personal Information and Sensitive Personal Information Due to Negligence
- Section 27 Improper Disposal of Personal Information and Sensitive Personal Information
- Section 28 Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
- Section 29 Unauthorized Access or Intentional Breach
- Section 30 Concealment of Security Breaches Involving Sensitive Personal Information
- Section 31 Malicious Disclosure
- Section 32 Unauthorized Disclosure
- Section 33 Combination or Series of Acts

5. Does the policy specify which data quality dimensions to be measured?

BSP implements IMF's Data Quality Assessment Framework with the following data quality dimensions:

- Assurance of integrity
- Methodological soundness
- Accuracy and reliability
- Serviceability
- Accessibility

6. Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?

Bank reports shall meet the reporting standards prescribed under Section 171 of the MORB. To ensure the quality of bank's reporting, Sanctions on reports for non-compliance with the reporting standards prescribes the corresponding sanctions for banks that fail to comply with such reporting standards. The Bangko Sentral shall conduct, as described under this Section on Assessment of reporting system, an assessment of the quality of a bank's reporting system in order to determine the underlying integrity of reports being submitted and root cause of persistent submission problems, if any.

For BSFIs, there is no specific data quality policy being enforced. However, internally, BSP is fully compliant with IMF's SDDS — Standards for Data Dissemination, and implements, IMF's DQAF — Data Quality Assessment Framework.

7. In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?

Under Basel Committee on Banking Supervision (BCBS) 239 Principles, there is a need to strengthen risk data gathering capabilities and internal risk reporting practices to enhance risk management and decision-making processes among banks.

ASEAN Model Contract Clauses (MCCs) and ASEAN Data Management Framework (DMF) are also adopted locally. NPC Advisory No. 2021 – 02 dated 28 July 2021 provides additional supplementary

[3] may be found in page 187 of Manual of Regulations for Banks

guidance as to how Personal Information Controllers and Personal Information Processors in the Philippines may use these standards in their respective personal data processing.

For BSP, international standards such as IMF's SDDS — Standards for Data Dissemination and IMF's DQAF — Data Quality Assessment Framework are adopted. For BSFIs, widely known certifications such as ISO/ IEC 27001 can provide requirements for an information security management system (ISMS).

The DCAM Framework by the EDM Council has also seen adoption.

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   This is part of the DPA of 2012 (Chapters V to VII), Section 148 on Information Technology (IT) Risk Management and Appendix 75 on IT Risk Management Standards and Guidelines, Area on Information Security of the MORB or the BSP IT Risk Management Standards and Guidelines, and Republic Act No. 10175 also known as the Cybercrime Prevention Act.

   The Banking Industry is required to adhere to Republic Act 10173 on the Data Privacy Act of 2012, which aims to maintain privacy of Personally Identifiable Information (PII) and includes provisions on processing, accountability for transfer, and security of personal information, and rights of the data subject, among others, including the corresponding breach reporting and penalty provisions for non-compliance.

   Meanwhile, Appendix 75 of Section 148 of the Manual of Regulations for Banks (MORB) and Appendix Q-62 of Sections 147-Q/ 145-S/ 142-P/ 126-N of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) lay down the framework to protect data and information throughout its life cycle.

   To further strengthen data breach prevention and control mechanisms, BSFIs are reminded of their responsibilities under Memorandum No. M-2021-043.

   BSP also issued guidelines covering technology and cyber-risk reporting and notification requirements for BSFIs for a more responsive, proactive and effective banking supervision.

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   There are several provisions in the mentioned regulations on risk detections, assessment, and response.

   According to Section 148 on Information Technology Risk Management, *an ISRM (Information Security Risk Management) framework should be in place encompassing key elements and phases with effective governance mechanisms to oversee the entire process.*

   The Framework involves a continuing cycle, comprising Identify, Prevent, Detect, Respond, Recover and Test.

   BSP has also issued recent policy reforms and ongoing cybersecurity initiatives, which include:

   - BSP Fraud Management Circular, which prescribes the adoption of fraud management systems to minimize losses arising from fraud and cyber-criminal activities
   - Memoranda on Retail Electronic Payment and Financial Services (EPFS) and API security, which recommend supplementary controls to thwart common electronic fraud, such as phishing and API-related attacks. Such provisions are initially issued as a discretionary guideline for the Banking Industry but is being incorporated in the upcoming amendment to regulations.

3. Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?

There are defined fines imposed by the regulators as stated in the law and related issuances.

Breach on security may lead to monetary and non-monetary sanctions and penalties such as revocation of license, sanctions to officers, and other enforcement actions. Meanwhile, data breaches include a provision for imprisonment in addition to applicable sanctions and penalties on the breach of security. Please refer to Chapter VIII of the DPA of 2012.

Singapore

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   - Personal Data Protection Act (PDPA)
   - Section 47 on Privacy of Customer Information and the Third Schedule on Disclosure of Information of the Banking Act 1970
   - Please also refer to the Data Security Section for the requirements and guidance related to data security
   - Domestic systemically important banks in Singapore are also expected to comply with BCBS 239 relating to data management, governance and quality of risk data.

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   Monetary Authority of Singapore (MAS) is responsible for the oversight/ enforcement of the Banking Act.

   The Personal Data Protection Commission (PDPC) is responsible for the oversight/ enforcement of PDPA.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   MAS has not issued any policies or guidance to Financial Institutions on data localisation.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. **what type of data is disallowed?**
   b. **which country(ies) for data storage is disallowed?**

   No.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

4. **What are the conditions to obtain the approval?**

   N.A.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

   N.A.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   While there is no explicit policy or guidance on cross border data sharing, there are banking regulatory requirements governing the disclosure of customer information. For instance, as per the PDPA requirements, transfers of personal data outside of Singapore requires the recipient of the personal data to provide safeguards equivalent to or greater than the requirements under the PDPA — this is outlined in Section 26(1).

   In addition, under the Banking Act, only under certain prescribed circumstances can customer's information be disclosed to a third party. For instance, customer gives written consent — this is outlined in the Third Schedule (Part 2) of the Banking Act

   Specific to the outsourcing of services by banks to service providers located outside of Singapore, there are also outsourcing requirements that govern the sharing of information between the service provider and the bank that has outsourced the services.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   No, conditions for the disclosure have been set out in the statutory provisions indicated under Q1.

   For the purposes of Section 26 of the Act, a transferring organisation must, before transferring an individual's personal data to a country or territory outside Singapore on or after 1 February 2021, take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations (in accordance with regulation 11) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   N.A.

4. **What is the process to obtain approval to share data?**

   A transferring organisation is taken to have satisfied the requirements of paragraph (1) in respect of an individual's personal data which it transfers to a recipient in a country or territory outside Singapore i

   (a) subject to paragraph (3), the individual consents to the transfer of the individual's personal data to that recipient in that country or territory;
   (b) the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data to that recipient under Section 15(3), (4), (5), (6), (7) or (8) of the Act;
   (c) the transfer of the personal data to the recipient is necessary for the personal data to be used or disclosed under Part 1 or paragraph 2 of Part 2 of the First Schedule to the Act, and the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose;
   (d) the personal data is data in transit; or
   (e) the personal data is publicly available in Singapore.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

6. **What are the conditions to obtaining the approval?**

   N.A.

7. **What government authorities are required to provide approvals?**

   N.A.

8. **What government interventions are needed to support cross border data storage?**

   N.A.

   However, to facilitate data sharing, MAS support would be required to work with the respective regulators to explore open standards like open banking[4], adoption of APEC CPBR etc.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Organisations in the banking industry must adhere to the Personal Data Protection Act (PDPA) which governs organisations' collection, use and disclosure of individuals' personal data. However, the provisions of banking sectoral laws or other written laws shall prevail if they are inconsistent with the provisions of the PDPA.

   The Advisory Guidelines for Key Concepts in the PDPA elaborate on and provide illustrations for the key obligations, and offer interpretation of key terms in the PDPA, which assist in organisations' understanding of the PDPA.

   Under Section 47 on Privacy of Customer Information of the Banking Act 1970 (BA), banks are prohibited from disclosing any customer information, except as permitted under the Third Schedule of the Act (e.g. where customer provides consent to the disclosure of his/ her personal data such as bank account information).

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   The PDPA does not define a category of sensitive personal data nor does it prescribe a standard on the levels of sensitivity of personal data.

   However, when enforcing the PDPA, the PDPC has considered certain types of data to be of greater sensitivity and should be accorded a higher degree of protection such as minor's data, NRIC data, financial and medical information. In addition, the Personal Data Protection (Notification of Data Breaches) Regulations 2021 prescribes a whitelist and categories of personal data that when breached, is more likely to result in significant harm to the individual. Whitelisted personal data relating to the banking industry includes individuals' account identifier, creditworthiness of an individual, outstanding debt of individual, etc. If such data under the whitelist is breached, the organisation must take the appropriate steps to notify the PDPC and/ or affected individuals.

[4] Open banking is a financial services term within financial technology. It refers to: the use of open APIs that enable third-party developers to build applications and services around the financial institution; greater financial transparency options for account holders, ranging from open data to private data; and the use of open source technology to achieve the above.

3. In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?

According to the PDPA, personal data refers to data, whether true or not, about an individual who can be identified (a) from that data or (b) from that data and other information to which the organisation has or is likely to have access. Nevertheless, the scope of personal data excludes business contact information. This can be found in Section 2 of the Act.

For the purposes of Section 47 of BA, customer information in relation to a bank refer to (a) any information relating to, or any particulars of an account of a customer of the bank, where the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customer; or (b) deposit information. This definition can be found in Section 40A.

4. What are the protection requirements (system-enabled) for personally identifiable information?

The Protection Obligation under the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. This is specified in Section 24 of the Act.

The Personal Data Protection Commission (PDPC) recognises there is no one size fits all solution for organisations to comply with the Protection Obligation, so each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances.

Some technical or system-enabled protection measures that organisations can adopt include ensuring computer networks are secure, adopting appropriate access controls (e.g. stronger authentication measures) and using the right level of email security settings when sending or receiving highly confidential emails.

5. What are the protection requirements (manual controls) for personally identifiable information?

Some physical measures or manual controls that organisations can adopt to protect personal data in their possession include storing confidential documents in locked file cabinets, restricting employee access to confidential documents on a need-to-know basis and properly disposing confidential documents that are no longer needs through shredding or similar means.

6. What are the restrictions on the use of PII data? How long are the restrictions for?

The Purpose Limitation Obligation under the PDPA limits or restricts the purposes for which and the extent to which an organisation may collect, use or disclose personal data. Specifically, organisations may only collect, use or disclose individuals' personal data only for purposes (a) that a reasonable person would consider appropriate in the circumstances, and (b) where applicable, that the individual has been informed of by the organisation. This is specified in Section 18 of the Act.

The Retention Limitation Obligation of PDPA prevents organisations from retaining personal data in perpetuity where it does not have legal or business reasons to do so. This is specified in Section 25 of the Act.

The Third Schedule of the BA permits disclosure of customer information by banks under specified circumstances.

7. Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.

The PDPA does not mandate organisation to perform data protection impact assessments, however performing a DPIA allows an organisation to identify, assess and address personal data protection risks based on the organisation's functions, needs and processes. In doing so, an organisation can better

assess if their handling of personal data complies with the PDPA, thus implementing appropriate measures to safeguard against data protection risks.

Click the link to access PDPC's Guide to Data Protection Impact Assessment.

8. **Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?**

Under the Consent Obligation of the PDPA, consent may be expressly obtained from the individual or deemed (e.g. when individual voluntarily provides their personal data or when it is required for fulfilling a contract).

The PDPA does not prescribe the exact way organisations collect personal data; however, it is recommended that organisations obtain individuals' consent in writing. Moreover, for the sending of direct marketing messages, organisations should obtain the express consent of individuals where individuals actively indicate their consent via an opt-in method. Organisations must allow for and facilitate the withdrawal of consent by the individual who has previously given, or deemed to have given, their consent.

Part One, Third Schedule of the BA permits disclosure of customer information by banks where the customer has provided consent in writing.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

While there are no explicit policies/ guidelines on data management, the Association of Banks in Singapore — Standing Committee on Data Management (ABS-SCDM), with guidance from MAS and IMDA, has developed a Data Sharing Handbook (Handbook), with the perspective of enhancing data sharing as part of data management. Part of the data sharing considerations include understanding the importance of metadata and ensuring data quality to enhance sharing effectiveness.

MAS Rules on reporting: Section 75B on Electronic service, 26 on Information to be provided by banks, 55ZD(1) of the Banking Act (Cap. 19); MAS Notice 610, 1003 Submission of Statistics and Returns and Notice.

In addition, the banking industry may refer to the following:

- Local Banks are committed to MAS to adopt BCBS 239 Standard for risk reporting
- Best practices: e.g., ABS data sharing handbook
- PDPC: Guide to Developing a Data Protection Management Programme
- Certification: IMDA Data Protection Trustmark (DPTM), IMDA APEC CBPR

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

BCBS 239: Principle 1 Governance – A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Basel Committee; Principle 2 Data Architecture and IT Infrastructure — 34. Roles and responsibilities should be established as they relate to the ownership and quality of risk data and information for both the business and IT functions.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

The handbook provides, for reference, common categories of data assets that banks generally have, as well as elements and importance of metadata and data quality.

The following resources are also available:

- ABS data sharing handbook: TYPES OF DATA
- BCBS 239: all 7 principles cover the data standards
- PDPC: Guide to Developing a Data Protection Management Programme Part 1: Governance and Risk Assessment: Risk Identification and Assessment — Confidentiality, Integrity and Availability (CIA).

4. Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?

Banking Act; Commitment to MAS – BCBS 239

There are no known penalties for non-compliance to BCBS 239, although MAS had handed out warning letters to banks which had noted errors in their regulatory submissions.

5. Does the policy specify which data quality dimensions to be measured?

The Handbook provides, for reference, a list of data quality dimensions typically used for assessment.

In addition, the banking industry may refer to the following:

- ABS data sharing handbook: TYPES OF DATA
- BCBS 239: Principle 3 Accuracy and Integrity; 4 Completeness, 5 timeliness, 6 adaptability, 7 accuracy

6. Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?

N.A.

7. In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?

Domestic systemically important banks in Singapore are expected to comply with BCBS 239 which is related to data management, governance and quality for risk data.

Other notable examples include:

- General: ISO 9001 Quality Management Systems, ISO 22301 Business Continuity Management Systems
- MAS: ISO20022 — electronic data interchange between financial institutions
- CSA: ISO/ IEC 15408 Common Criteria, ISO/ IEC 27001 Information Security Management System (ISMS), ISO/ IEC 27031 Information technology–Security techniques–Guidelines for information and communication technology readiness for business continuity, ISO/IEC 20117:2004 Information technology – Telecommunications and information exchange between systems. IEC 62443-3 Industrial communication networks –Network and system security–Part3-3: System security requirements and security levels, 2013
- PDPC: DPTM — ISO27001 ISMS; Guide To Securing Personal Data In Electronic Medium, ISO/ IEC29100 privacy principles; ISO/ IEC 27018 privacy principles for the public cloud computing environment, ISO27701 Privacy Information Management System (PIMS)
- Data Governance Frameworks: ISO/ IEC 38505-1:2017 Information technology – governance of data, Control Objectives for Information Technologies (COBIT) 2019, ISO/ IEC 38500 Information technology – Governance of IT for the organisation, and ISO/ TC 215 Health informatics

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   MAS sets out minimum requirements and guidance on technology risk management (TRM), including data security, in notices and guidelines, as well as through the issuance of circulars and advisories.

   For example, the TRM Notice imposes legally binding requirements on FIs to implement IT controls to protect customer information from unauthorised access or disclosure.

   MAS has also issued a Cyber Hygiene Notice which requires FIs to implement a set of fundamental controls to mitigate the most common and pervasive cyber security risks today and raise their overall level of cyber resilience.

   The TRM Guidelines set out risk management principles and best practices to guide FIs to establish a robust TRM framework, strengthen cyber security controls, implement strong authentication to protect customer data, and monitor and respond to cyber threats.

   MAS also issues circulars and advisories to remind FIs to manage emerging IT risks. For example, MAS has issued circulars and advisories to alert FIs on phishing campaigns and remind them to be vigilant against prevailing cyber threats.

   More general policies include Cybersecurity Act 2018 and Computer Misuse Act (CMA).

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   See response to Question 1 on Data Security.

3. **Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?**

   The penalty for a breach of the TRM or Cyber Hygiene Notice can range from $100,000 for Banks and Insurance companies, to $150,000 for Exchanges. MAS has the powers to take other supervisory actions, including, requiring FIs to set aside additional regulatory capital until MAS is satisfied that adequate technology risk control measures have been put in place to address deficiencies.

   Should the cyber security breach also result in a contravention of Section 47 of the Banking Act (i.e. Customer information is disclosed for purposes that have not been provided for under the Act) the persons responsible shall be guilty of an offence and shall be liable on conviction

   i) in the case of an individual, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or
   ii) in any other case, to a fine not exceeding $250,000.

   - Cybersecurity Act 2018

     Fines not exceeding SGD 10,000 for each contravention or non-compliance which is not an offence, but not exceeding SGD 50,000 in aggregate.

     Criminal sanctions: Varies depending on the specific offence, although in general a criminal fine not exceeding SGD 100,000 or imprisonment for a term not exceeding two to ten years or both.

   - CMA

A criminal fine not exceeding SGD 50,000 or imprisonment for a term not exceeding ten years or both; and

In respect of protected computers, a criminal fine not exceeding SGD 100,000 or imprisonment for a term not exceeding 20 years or both. Compensation for damage caused to computer, programme or data.

Thailand

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   There are no explicit directives against general data sharing of which I am aware. However, there are legislations that effectively render data sharing somewhat difficult if not illegal unless done through a very specific mechanism.

   a) Credit Business Information Act of 2002 (CBIA) generally permits credit information sharing but only through the National Credit Bureau (NCB). That is not entirely true. Any Thai company can apply for approval to be in credit business information business. But the reality is that the law was designed to create a single bureau, the Thai National Credit Bureau. This makes sharing of credit data by other means illegal.
   b) The CBIA above also mandates that processing of credit information must be done domestically. Processing under the act is defined so broadly that any transmission of credit information to destination outside the Kingdom is illegal.
   c) Personal Data Protection Act of 2019 is modelled after EU GDPR and contains provisions very similar to those found in GDPR. The act itself does not explicitly rule out cross border data sharing. Though it requires that the destination countries are under similarly stringent data protection regime and the data processors in foreign countries are deemed adequately certified. Details of the Act implementation are supposed to be codified in other supporting directives and regulations.
   d) There are other general business-related acts, including Thailand Public Company Act and those related to publicly traded entities and anti-trust regulations that contains provisions restricting sharing of companies' data with external parties out of one type of concerns or another. To be fair, these restrictions apply equally to sharing with domestic parties and those abroad.

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   a) The Act enforcement falls under the purview of Ministry of Finance. But NCB itself is regulated by Credit Information Protection Committee. The committee is chaired by Bank of Thailand (BOT) governor with members from various organizations including representatives from the banking association. The secretariat function, however, is performed by BOT, thus rendering all credit information sharing effectively a sole province of BOT.
   b) 1.2. PDPA — The Act creates an oversight committee, the Personal Data Protection Committee and the office of Personal Data Protection Committee (PDPC) with duties to produce directives and oversees their implementation. Unfortunately, much of the supposed frameworks, directives, and procedures are still in discussion so we cannot be certain that restrictions on cross border sharing are on the table or not.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   We are not aware of any specific localization restrictions with the sole exception being the one contained in the CIBA which mandate strict localization of credit information processing.

   CIBA generally permits credit information sharing but only through the NCB. That is not entirely true. Any Thai company can apply for approval to be in credit business information business. But the reality is that the law was designed to create a single bureau, the Thai NCB. This makes sharing of credit data by other means illegal.

The CBIA above also mandates that processing of credit information must be done domestically. Processing under the act is defined so broadly that any transmission of credit information to destination outside the Kingdom is illegal.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
    a. **what type of data is disallowed?**
    b. **which country(ies) for data storage is disallowed?**

    As per Question 1.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

    N.A.

4. **What are the conditions to obtain the approval?**

    N.A.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

    N.A.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

    If the question focuses on explicit restrictions on data sharing, cross border or otherwise then the answer is no. We are unaware of any such explicit restriction.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

    As above.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

    The type of data, objective and necessity of the sharing data must be discussed first.

4. **What is the process to obtain approval to share data?**

    N.A.

5. **Is there an estimated timeframe to which such approvals are obtained?**

    N.A.

6. **What are the conditions to obtaining the approval?**

    N.A.

7. **What government authorities are required to provide approvals?**

   N.A.

8. **What government interventions are needed to support cross border data storage?**

   N.A.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Personal Data Protection Act of 2019 is modelled after EU GDPR and contains provisions very similar to those found in GDPR. The act itself does not explicitly rule out cross border data sharing. Though it requires that the destination countries are under similarly stringent data protection regime and the data processors in foreign countries are deemed adequately certified. Details of the Act implementation are supposed to be codified in other supporting directives and regulations.

   The Act creates an oversight committee, the Personal Data Protection Committee and the office of Personal Data Protection Committee (PDPC) with duties to produce directives and oversees their implementation. At present, there are six secondary legislations published in Krisdika website.

   However, much of the supposed frameworks, directives, and procedures are still in discussion so we cannot be certain that restrictions on cross border sharing are on the table or not.

   The BOT would like to add that currently Thailand's Office of the Council of State has published six secondary legislations in their website.

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   Though there are no national standards that explicitly written in the Act, during the public communication, PDPC explained that personal data may be separated into 2 parts:

   a. Personal data: any information relating to a Person, which enables the identification of such Person, whether directly or indirectly, but not including the information of the deceased Persons.
   b. Sensitive Personal Data: the subset of the Personal data that may lead to discrimination such as racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner as to be prescribed by the PDPC.

3. **In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?**

   The act identifies the followings as sensitive information

   a) Race
   b) Nationality
   c) Religious belief
   d) Political view
   e) Sexual orientation
   f) Criminal record
   g) Health information
   h) Labour union membership
   i) Biometric information

The act would "catch all", i.e. anything that might impact the data subject and enable the identification of such Person, whether directly or indirectly.

4. What are the protection requirements (system-enabled) for personally identifiable information?

Currently, there are no protection requirements that explicitly written in the Act. However, the principles of personal data protection can preliminarily be summarized as follows: (1) lawfulness, fairness and transparency (2) purpose limitation (3) data minimization (4) accuracy (5) storage limitation (6) integrity and confidentiality and (7) accountability.

Data owner is indicated as having responsibilities to:

a) Ensure secure storage
b) Safeguard against unauthorized access
c) Provide for deletion of PII
d) Notification of data breaches
e) Establish domestic representative
f) Maintenance of record of processing.

5. What are the protection requirements (manual controls) for personally identifiable information?

The act makes no distinction between system and manual controls.

6. What are the restrictions on the use of PII data? How long are the restrictions for?

BOT views that under the PDPA laws, the Data Controller shall not use or disclose Personal Data without the consent of the data subject, unless it is the Personal Data which is collected without requirement of consent such as Legal Obligation, Legitimate Interest, Public Task undersection, Vital interest, Research. Therefore, the data controller must obtain the consent from the data subject before using or disclosing personal data and the data subject has the right to withdraw his or her consent at any time.

The act is designed under permission-based regime, meaning that it prescribes when PII can be used with exemptions mostly related to public safety, law enforcement, act of parliaments, etc. The use outside of the prescription is therefore illegal. The act does not identify protection roll-off mechanism, which suggest that it is not time-bound.

7. Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.

Currently, the impact assessment mechanism is not part of the Act.

However, in banking industry, the Thai Bankers Association (TBA) has developed the Guideline on Personal Data Protection for Thai Banks to layout practices in compliance with the PDPA law and there is a topic about the data protection impact assessment (DPIA) and its procedure which quoted from the principles of EU GDPR law.

8. Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?

Though there is no standard on consent forms or mechanisms prescribed, important principles of requesting for the consent are as follows:

- The Data Controller shall not collect, use, or disclose Personal Data, unless the data subject has given consent prior to or at the time of such collection, use, or disclosure.
- A request for consent shall be explicitly made in a written statement, or via electronic means
- In requesting consent from the data subject, the Personal Data Controller shall also inform the purpose of the collection, use, or disclosure of the Personal Data.

- Such request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an easily accessible and intelligible form and statements, using clear and plain language, and does not deceptive or misleading to the data subject in respect to such purpose.
- the Data Controller shall utmost consider that the data subject's consent is freely given.
- The data subject may withdraw his or her consent at any time.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   Please refer to the policy guideline on Data Governance (BOT).

   In addition, PDPC is supposed to produce guidance on the issues but have yet to do so. BOT has issued guidance on the matter.

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   BOT guidance does not identify data function as such. Rather, the guidance identifies roles and responsibilities within the organization that should be in place. Further, it suggests how these roles and responsibilities should be assigned to various units and functions within the organization.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   At the time being, no policy is mentioning the minimum data standards that are required to be adhered to.

4. **Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?**

   BOT circular on the matter is a guidance on data governance. Consequences of non-compliances should not rise to the same level as breaches of directives. However, persistent non-compliances are deemed weaknesses therefore contribute to the outcome of the bank's periodic examination process. BOT may choose to issue a specific directive to the offending bank demanding its compliance and therefore upgrading its impact to the same level as other BOT directives, thus carrying the weight and penalty under the banking act. At which point, the failure to comply with the subsequent directive to achieve compliance with the guidance is now subject to the usual penalties.

5. **Does the policy specify which data quality dimensions to be measured?**

   The guidance describes the necessity of having a data standard. But it stops short of prescribing its nature. Though it does provide an example of what constitute good quality data. The features of good quality data are complete, accurate, up-to-date, consistent, not-redundant, and ready-to-use.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   No.

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   Not applicable.

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   BOT has a few out, including:

   a) Cyber Resilience Assessment Framework v.2
   b) Guiding Principles for Mobile Banking Security
   c) Guidelines on the use of Biometric Technology in Financial Services
   d) Supervisory Guidance on IT Risk Management
   e) Guidelines for Performing iPenTest

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   All the guidelines above contain various prescriptions on detection, assessment, and response to cyberthreat, though not necessarily specific to data security. Note that data security is often called out as consequences of cyberthreat in various places.

3. **Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?**

   As per the BOT, the penalty on failure to comply with PDPA is as follows;

   a) Civil penalties: the data subject can claim actual compensation and the court has power to sentence the data controller or data processor to pay punitive damages not exceeding two times the amount of the actual compensation;
   b) Administrative fines include monetary fines up to 5 million baht;
   c) Criminal penalties include up to 1 year of imprisonment of liable corporate officers or up to 1 million baht monetary fines or both.

   However, do note that BOT guidance on cyber security does not go into the specific about penalties associated with cyberthreat breaches. The penalties outlined above apply only when the bank is proven to have failed in complying with PDPA rather than as a response to specific data breaches.

Vietnam

General

1. **What are the key regulatory requirements on data that are being enforced in your country? Please specify the notice(s) and/ or reference number(s).**

   The key regulatory requirements on data that are being enforced in our country:

   a) The Civil Code Law No. 91/ 2015/ QH13;
   b) Law on Network Information Security No. 86/ 2015/ QH13 dated November 19, 2015;
   c) Law on Cyber Security No. 24/ 2018/ QH14 dated June 12, 2018;
   d) Law on Information Technology No. 67/ 2006 / QH11;
   e) Law on Electronic Transactions 2005 No. 51/ 2005/ QH11;
   f) Law on Consumers Protections No. 59/ 2010/ QH12, dated November 17, 2010;
   g) Law on Credit Institutions No. 47/ 2010/ QH12 dated June 16,2010;
   h) Law on Access to Information 2016 No. 104/ 2016 / QH13;
   i) Law on Protection of State Secrets No. 29/ 2018 / QH14 dated November 15, 2018;
   j) Law on Anti-Money Laundering (AML) No. 07/ 2012/ QH13 dated June 18,2012;
   k) Decree No. 85/ 2016 / ND-CP dated 01/ 07/ 2016 of the Government on security of information systems by level;
   l) Decree No. 117/ 2018/ ND-CP dated September 11, 2018 of the Government on protection of confidentiality and provision of client information of credit institutions, foreign bank branches.
   m) And documents guiding the above-mentioned Laws.

2. **Please specify the government organisation responsible for oversight / enforcement of these regulatory restrictions/ requirements.**

   - The Ministry of Information and Communication of Vietnam performs state management on information; electronic information; data and etc. (Decree 17/ 2017/ ND-CP stipulates the functions, tasks, powers and organizational structure of the Ministry of Information and Communications).
   - The Ministry of Public Security of Vietnam oversees cybersecurity (Law on Cyber Security).
   - In addition, other relevant ministries manage information and data within their respective sector.

Data Sovereignty / Localisation

1. **Are there any data sovereignty / localisation related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   The Article 26.3 of Law on Cyber Security stipulates: *Domestic and foreign service providers on telecom networks and on the internet and other value added services in cyberspace in Vietnam (cyberspace service provider) carrying out activities of collecting, exploiting (using), analysing and processing data (being) personal information, data about service user's relationship and data created by service users in Vietnam must store data in Vietnam for a period stipulated by the Government.*

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the storage of data outside of your country? If yes:**
   a. what type of data is disallowed?
   b. which country(ies) for data storage is disallowed?

   No, except data as specified in the Law on Protection of State secrets.

3. **What is the process to obtain approval to share copies of the data? Is there an estimated timeframe to which such approvals are obtained?**

   The process to obtain approval to share copies of state secret data in the banking sector is specified in the State Secrets Protection Regulation of the State Bank of Vietnam (SBV) that was issued together with Decision No. 2251/ QD-NHNN dated December 28, 2020 of the SBV.

   In case of sharing customer information data, the order and procedures for providing customer information are specified in the Government's Decree No. 117/ 2018/ ND-CP dated September 11, 2018 on confidentiality and provision of customer information of credit institutions, foreign bank branches.

   This Decree prescribes detail about storage and confidentiality of client information at banks. Specifically, Banks may only provide client information in 2 cases:

   i. Other organizations and individuals have the right to request banks to provide client information as prescribed in the National Assembly's codes, laws and resolutions;
   ii. When the provision of information is approved by clients.

   - Banks may not provide any agencies, organizations or individuals with client authentication information for accessing banking services (including clients' security codes, biometric data, access pass codes…) unless such provision is approved in writing by or in other forms as agreed upon with such clients;
   - State agencies, other organizations and individuals may only request banks to provide client information for proper purposes, with contents, and within the scope and competence as prescribed by law or as agreed upon by the clients and shall take responsibility for such request;
   - State agencies, other organizations and individuals that request provision of client information shall keep confidentiality of such information and use it for proper purposes, and may not provide the information to any third party without the clients' consent, unless the information is provided under law.
   - This Decree also prescribes that clients have the rights to lodge complaints, initiate lawsuits or request compensation for damage under law in case state agencies, other organizations, individuals, credit institutions or foreign bank branches provide or use client information in contravention of law.

4. **What are the conditions to obtain the approval?**

   N.A.

5. **What is/ are the names of the government authority(ies) that grant the approvals?**

   N.A.

Cross Border Data Sharing

1. **Are there any cross border data sharing related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   The Law on Cyber Security but there are no specific policies guidance issued.

2. **Does your country's Banking Act or other regulations (e.g. cybersecurity law) expressly disallow the sharing of data outside of your organisation / country?**

   N.A.

3. **If your answer to Question 2 is "Yes", what are the specific types of data that are being prevented from flowing out of the country?**

   N.A.

4. **What is the process to obtain approval to share data?**

   N.A.

5. **Is there an estimated timeframe to which such approvals are obtained?**

   N.A.

6. **What are the conditions to obtaining the approval?**

   N.A.

7. **What government authorities are required to provide approvals?**

   N.A.

8. **What government interventions are needed to support cross border data storage?**

   N.A.

Personal Data Privacy

1. **Are there any data privacy related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   - Articles 14.2, 14.3 of Law on Credit Institutions 2010 (amended and supplemented) stipulates that *credit institutions must ensure the confidentiality of information relating to accounts; deposits, deposited assets and transactions of customers at Credit institutions (CIs), foreign bank branches; CIs are not allowed to provide information relating to the account; deposits, deposited assets, and transactions of customers at the credit institution for other institution, individuals, unless requested by a competent state-bodies; in accordance with the law or with the consent of the customer* ;
   - Law on protection of consumers No. 59/ 2010/ QH12 (Articles 6.1);
   - Decree No. 117/ 2018/ ND-CP dated September 11, 2018 of the Government on protection of confidentiality and provision of client information of credit institutions, foreign bank branches (Articles 4.2, Article 13);
   - Decree on personal data protection is currently being drafted by the Ministry of Public Security;
   - Circular 39/ 2014/ TT-NHNN of the SBV dated 28/ 01/ 2013.

2. **Are there any national standards set to the levels of sensitivity of personal data? If so, what are these levels?**

   There are no provisions on sensitive levels of personal information but there is definition of information such as: bad debt; breach of payment obligation; violations law; lawsuit; prosecuted; prosecuted and other unfavourable information affecting the results of the borrower's solvency assessment specified in Clause 9, Article 3 of Circular No. 03/ 2013/ TT-NHNN January 28, 2013 of the Governor of the SBV that stipulating on the credit information activities of the SBV (as amended and supplemented).

   Decree on personal data protection is currently being drafted by the Ministry of Public Security of Vietnam.

3. **In accordance to the regulations, what constitutes as personal data / personally identifiable information (PII) in your country?**

   Personal data is defined in Clause 1, Article 9 of the Law on Citizen's Identity.

   In the banking sector, customer information of credit institutions and foreign bank branches is defined in Clause 1,2, Article 3 of Decree No. 117/ 2018/ ND-CP:

a) Customer information of CIs, foreign bank branches (hereinafter referred to as customer information) is information provided by customers, information arising in the process of customers' request or provided by CIs, foreign bank branches on banking operations, products and services in permitted activities, including customer identification information and the following information: account information, information on deposits, information on deposited properties, information about transactions, information about organizations and individuals being a securing party at credit institutions, foreign bank branches and relevant information other.
b) Customer identification information is the following information: a) For individual customers: full name, signature sample, electronic signature, date of birth, nationality, occupation, address of permanent residence, current address, foreign register address, phone number, email address, number, date of issue, place of issue of identity card or citizenship card or passport (visa information for individual customers who are foreigners) of customers or of legal representatives or authorized representatives (collectively referred to as legal representatives) and other relevant information; b) For entities: full transaction name, abbreviated name, license or establishment decision, enterprise registration certificate or equivalent document; head office address, phone number, fax number, email address and information specified in point a of this clause of the legal representative and other relevant information.

In addition, personal information is information that identifies the customer and the following information: account information, information about deposits, information about deposited assets, information about transactions and information available. Other related matters (Clause 3 Article 4 of Circular No. 09/ 2020/ TT-NHNN).

4. What are the protection requirements (system-enabled) for personally identifiable information?

Requirements for information protection (on a system basis) for personally identifiable information (in the banking sector) are specified in Circular No. 09/ 2020/ TT-NHNN (including requirements for updating information systems, requirements for managing of internet connection, …).

5. What are the protection requirements (manual controls) for personally identifiable information?

Requirements for information protection (manual control) for personally identifiable information (in the banking sector) are not specified.

6. What are the restrictions on the use of PII data? How long are the restrictions for?

N.A.

In principle, citizens are guaranteed personal and family information secrets in the National Population Database and Citizen Identification Database, except cases subject to provision of information and documents as prescribed by law (Point a, Clause 1, Article 5 of the Law on Citizen Identification).

In the banking sector, the client information of the credit institutions, foreign bank branches must be kept confidential and provided only in accordance with the Law on Credit Institutions (as amended and supplemented), this Decree and relevant laws (Clause 1, Article 4 of Decree No. 117/ 2018 / ND-CP)..

7. Are there any requirements to perform data protection impact assessments (DPIA) or similar risk assessments? If yes, please share the document / link to the website.

The assessment of information security is specified in Article 42 of Circular No. 09/ 2020/ TT-NHNN.

8. Under the regulations / law, how is the consent obtained from the data subjects prior to the use of personal data?

Article 14.3 of the Law on Credit Institutions 2010 (amended and supplemented) and Article 11 of Decree No. 117/ 2018/ ND-CP.

Data Management

1. **Are there any data management, governance and quality related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   As stipulated in Article 14, Law on Credit Institutions (amended and supplemented) CIs are not allow to provide information relating to customers' accounts, deposits, deposited assets and transactions at credit institutions to other organizations and individuals, unless otherwise requested by competent state agencies as prescribed by law or approved by customers.

   - Law on AML stipulates information storage under the confidentiality regime;
   - Law on Cyber Security No. 24/ 2018 / QH14 dated 12/ 06/ 2018;
   - Law on Internet Information Security No. 86/ 2015 / QH13 dated November 19, 2015
   - Decree 85/ 2016 / ND-CP dated 01/ 07/ 2016 on security of information systems by level

   Documents applicable to the State Bank of Vietnam (SBV):

   - Decision No. 2728/ QD-NHNN of the SBV dated December 31, 2019 on Promulgating the State Bank's Information Security Risk Management Framework
   - Decision No. 1820/ QD-NHNN of the SBV dated October 26, 2020 on SBV's regulations on information safety and confidentiality

   Documents applicable to credit institutions:

   - Circular No. 09/ 2020/ TT-NHNN of the SBV dated October 21, 2020, regulations on information system safety in banking operations that applied for CI, foreign bank branches, payment intermediaries, credit companies, asset management companies
   - Circular No. 47/ 2014/ TT-NHNN of the Subedited December 31, 2014, technical requirements on safety and security with equipment for bank card payments
   - Circular No. 35/ 2016/ TT-NHNN of the SBV dated December 29, 2016, regulations on safety and confidentiality for the provision of internet banking services
   - Circular No. 03/ 2013/ TT-NHNN of the SBV dated 28/ 01/ 2013, the processing, keeping and keeping confidential credit information data (Article 9)
   - Circular No. 09/ 2020 / TT-NHNN: Chapter II, Section 4: Operation management and information exchange, Article 22: Backup; Section 6: Management of the use of third party on information technology services, Article 35: Service contract with the third party

2. **Does the policy mention the roles and responsibilities of the data function? If yes, please provide the policy and section.**

   - Decree No. 85/ 2016/ ND-CP of the Government dated 01/ 07/ 2016 on security of information systems by level
   - Circular No. 09/ 2020/ TT-NHNN of the SBV, Chapter I, Article 4: Classification of information
   - Circular No. 09/ 2020/ TT-NHNN, Chapter I, Article 5 of the SBV: Classification of information systems.

3. **Does the policy mention minimum data standards that are required to be adhered to? If yes, please provide the policy and section.**

   N.A.

4. **Is the policy / guidance enforceable by law? If yes, what are the penalties for non-compliance?**

   Clause 4, Article 9 of Circular 03/ 2013/ TT-NHNN of the SBV dated 28/ 01/ 2013: *Credit information data must be kept confidential, ensuring no illegal access under this Circular and other provisions of Laws*.

- Penalties imposed on breaches: VND 20 million to VND 40 million for one breach.
- Circular No. 03/ 2013/ TT-NHNN dated January 28, 2013 of the Governor of the SBV that stipulating on the credit information activities of the SBV (as amended and supplemented). Article 9: Processing, storage and protection of confidential credit information data;
- Decree No. 88/ 2019/ ND-CP of the Government dated November 14, 2019 on penalties imposed for administrative violations in the monetary and banking sector: (i) Article 19. Violations of regulations on collection and processing of credit information; and (ii) Article 20. Violations of regulations on safety and credit information storage of credit information.

5. **Does the policy specify which data quality dimensions to be measured?**

   N.A.

6. **Have minimum standards on data quality been defined? If so, what are these? If not, what is the acceptable standards required by your regulators?**

   Data that lack standards i.e. wrong forms, lack of required information criteria, duplicate information or other technical errors which be returned partially or fully of error data by the Credit Information Centre of the SBV.

   Data adjustments are stipulated in Article 17: Adjust error data in Circular No. 03/ 2013/ TT-NHNN dated January 28, 2013.

7. **In countries with an absence of local governance regulations on data governance, are there any adoption of international standards for management of data? If so, what are these?**

   N.A.

Data Security

1. **Are there any data security related policies or guidance documents issued in your country that the banking industry must adhere to? If yes, please share the document / link to the website.**

   - The Law on Credit Institutions 2010 (amended and supplemented) stipulates that credit institutions must ensure the confidentiality of information relating to accounts; deposits, deposited assets and transactions of customers at credit institutions, foreign bank branches; Credit institutions may not provide information relating to the account; deposits, deposited assets, and transactions of customers at the credit institution for other institution, individuals, unless requested by a competent state-bodies; in accordance with the law or with the consent of the customer (Articles 14.2, 14.3);
   - Law on Internet Information Security No. 86/ 2015 / QH13 dated November 19, 2015;
   - Law on Cyber Security No. 24/ 2018 / QH14 dated 12/ 06/ 2018;
   - Decree 85/ 2016 / ND-CP dated 01/ 07/ 2016 on security of information systems by level;
   - Decree No. 117/ 2018/ ND-CP of the Government dated September 11, 2018 of the Government on protection of confidentiality and provision of client information of credit institutions, foreign bank branches.
   - Circular No. 09/ 2020/ TT-NHNN of the SBV dated 21/ 10/ 2020 Regulation on the security of information systems in banking operations.

2. **Does the policy address risk detection, assessment and response to cyberthreats on data security? Please provide details and links to the document / website**

   - The Law on Cyber Security contains regulations on prevention, detection and handling of cyber security breaches;
   - Decree No. 25/ 2014/ ND-CP dated April 7, 2014 of the Government on prevention of crime and other violations of laws on using high technology with regulations on detection, handling of crimes. and other law violations of using high technology.

3. Are there penalties imposed on cyber security breaches that result in data loss? What are the penalties for the breach of such security?

N.A. The Decree on penalties imposed on administrative violations of cyber security is being developed by the Ministry of Public Security.

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.