ASIFMA JURISDICTIONAL COMPARISON OF DATA PROTECTION RULES

A comparison of key data protection regulation across APAC jurisdictions

JULY 2020

Developed in kind collaboration with:
<table>
<thead>
<tr>
<th>Country</th>
<th>General data privacy and protection laws and regulations</th>
</tr>
</thead>
</table>
| China           | The Cybersecurity Law of the People’s Republic of China (the “CPL”); the “NIP” was released by the Standing Committee of the National People’s Congress and came into force on October 20, 2017. Regulations issued by the Ministry of Industry and Information Technology (MIIT) and the National Information Security Bureau, and the Multiple Level Protection System of Information Technology Software and Systems (the “MLP System”) are generally referred to as “NIP”.
| India           | The Personal Data Protection Act (PDPA) was enacted in 2019, and is administered by the Personal Data Protection Commissioner (the “PDPC”). The PDPC is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Hong Kong       | The Personal Data Protection Ordinance (the “PDPO”) was enacted in 1996, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPO.
| Singapore       | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Malaysia        | The Personal Data Protection Act (PDPA) was enacted in 2010, and is administered by the Personal Data Protection Commissioner (the “PDPC”). The PDPC is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Thailand        | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Personal Data Protection Commissioner (the “PDPC”). The PDPC is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Indonesia       | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Philippines     | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Vietnam         | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Japan           | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Korea           | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| Australia       | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.
| New Zealand     | The Personal Data Protection Act (PDPA) was enacted in 2012, and is administered by the Commissioner of Personal Data Protection (the “PCPP”). The PCPP is responsible for enforcing the PDPA. The MLP System is the basis for implementing the PDPA.

The General data privacy and protection laws and regulations framework is available here. The ASIAN framework on data protection is available here.
The Chinese banking and insurance regulatory body, the CBIRC (China Banking and Insurance Regulatory Commission, previously known as the CBRC), has issued a series of measures to protect the privacy of personal financial information. These measures, which extend beyond the Banking Act of 2008, are designed to strengthen the protection of consumer rights and ensure the safe and secure handling of personal data.

### Personal Financial Information Protection

- **Institutions only.**
- **Personal or critical regulation on third parties.**

Institutions are required to establish a procedure for the handling of personal financial information, including the protection of data during and after any transaction. This procedure must include the following:

1. **Protecting Personal Financial Information:** Any institution that collects, stores, or processes personal financial information must implement appropriate measures to protect this data from unauthorized access, use, or disclosure.
2. **Regulating Financial Information:** Institutions must ensure that all staff are trained in the regulations regarding the protection of personal financial information.
3. **Prudential Guidelines:** Prudential guidelines issued by the CBIRC cover the management of personal financial information. These guidelines are designed to ensure that institutions maintain robust and effective cybersecurity controls to protect the data of the bank's customers.
4. **Technology Risk:** The CBIRC has issued guidelines on data protection, which contain relevant provisions under regulations by the PBOC (People's Bank of China) and the CSRC (China Securities Regulatory Commission).
5. **Privacy Act 1988:** The Privacy Act 1988 must be complied with under GDPR (General Data Protection Regulation) guidelines.
6. **Privacy Commissioner:** Businesses, agencies, or types of personal information that need to be followed under existing industries and agencies or types of personal information that need to be followed under existing industries and agencies.

### Colonial Circular to Emphasize Banking on Financial Information Protection

A circular issued by the Banking Association in January 2013 emphasizes the importance of protecting personal financial information. This circular is meant to ensure that institutions comply with the regulatory requirements and to set out the responsibilities of the Bank, the Methodist Church, and the financial institutions in place to protect the data of their customers.

### Financial Information Protection

- **The Circular on the Banking on Financial Information Protection:** The Circular on the Banking on Financial Information Protection (Circular Number 2013/488) was issued on 14 March 2013.

This circular provides a framework for banks to manage and protect personal financial information. It includes guidelines for the handling of personal financial information, including the identification of sensitive data, the implementation of data protection measures, and the responsibilities of the bank, the Methodist Church, and the financial institutions.

### Conclusion

The protection of personal financial information is a critical aspect of banking in Malaysia, and institutions are required to implement robust measures to protect the data of their customers. This includes the establishment of a formal procedure for the handling of personal financial information, the implementation of appropriate security controls, and the training of staff in the regulations governing the protection of personal financial information.
In addition, the legislative bodies in the UK cannot be expected to change following the expiration of the Brexit “transition period” at the end of the year. It is considered does not have to clarify which data subjects a data subject’s right to data breach notification is subject to significant harm or data breach notification when it occurs. The draft Bill requires a controller to notify the individuals to which the personal data relates. Information on the public interest or in the public interest to the right and freedom of any person. In addition, the exempted data breaches likely to cause significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Information and Communication Technology (the “MOCI”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach
type remarkable data protection in Indonesia. Currently, personal data protection in Indonesia is governed by several regulations. Much of the draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.

The Ministry of Industry and Information Technology (the “MIIT”) has also indicated that the Ministry will change the implementation of certain provisions in the Act. The Ministry is also currently considering the proposal for the Amendment proposals for breach notification. It is not reasonably required to report a data breach to the UK on recipient data is subject to further investigation. The draft Bill provides that the personal data is subject to significant harm or data breach notification.
| No. | Proposed new financial services sector rule | China | India | Hong Kong | Singapore | Malaysia | Thailand | Indonesia | Philippines | Vietnam | Japan | Taiwan | Australia | New Zealand |
|-----|--------------------------------------------|-------|-------|-----------|-----------|----------|----------|----------|-----------|----------|-------|-------|---------|------------|-------------|
| 4.  | Proposed new financial services sector rule (e.g. Confidentiality, Information Security, Bank Secrecy, including relating to intercompany third-party transfers) | None | None | None | None | None | None | None | None | None | None | None | None | None |
|     | As reported, the PBOC recently prepared a draft of the Interim Measures for the Protection of Personal Financial Information, which proposed new measures to protect Chinese financial institutions in October 2019. These measures may be intended to enhance financial institution intercompany reliance with a focus on governance and management. The Payment Services Act has commenced on 28 Jan 2020. | None | None | None | None | None | None | None | None | None | None | None | None | None |

As reported, the PBOC recently prepared a draft of the Interim Measures for the Protection of Personal Financial Information, which provided draft measures to certain Chinese financial institutions in October 2019 for consultation. These draft measures may apply to the collection, processing, use, and disclosure of personal financial data by various financial institutions in China. These measures, when finalized, are intended to enhance financial institution intercompany reliance with a focus on governance and management.

The PBOC released a new draft of the Implementation Measures for the Protection of Rights and Interests of Financial Consumers on December 27, 2019 (the "Draft Implementation Measures"). The Draft Implementation Measures aim to replace (i) the Implementation Measures for the Protection of Rights and Interests of Financial Consumers that were issued by the PBOC and came into force on 14 December 2016 and (ii) the Administrative Measures for the Protection of Rights of Financial Consumers (Trial) that were issued by the PBOC and came into force on 7 May 2013. The Draft Implementation Measures reiterate data storage and processing localization requirement as well as other protection obligations of financial institutions in terms of their processing of consumer financial information.

Changes to the Credit Reporting Privacy Code (Amendment No. 14) were made in three stages in 2019, following a 18-month review into the operation of the comprehensive credit reporting system. These changes were intended to enhance the credit reporting system's fairness for consumers and improve enforcement and compliance.

Amendment No. 14 changes came into force on three phases on 1 July, 1 April, and 1 October 2019. The latest changes increased the threshold for listing overdue payments as defaults in credit reports. It also obliges credit providers to cease quotation inquiries when offering risk-based pricing for credit products.

Changes to the Superannuation Schemes Unique Identifier Code (Amendment No. 1) were made in three stages in 2019. The Code has been amended by Amendment No. 1 and commenced on 15 October 2015. Amendment No. 1 will make two minor changes to the Code. Firstly, it will amend the definition of the term "associated person" to replace a reference to section 587 of the Income Tax Act 1994 (which has since been repealed) with its current equivalent – paragraph 106 of the Income Tax Act 2007. Secondly, it will remove clause A2. This clause will not be extended or extended to new or existing entities and express prescribing in the Code but which are defined by the Privacy Act 1993 or Acts Interpretation Act 1901 which is the current equivalent to Acts Interpretation Act 1901. As at the date of this summary table, there is no concrete proposal for additional data privacy and protection rule.

None | N/A | None | None as at the date of this summary table | None | None | None | None | None | None | None | N/A | No information found that is released by the Reserve Bank of New Zealand (RBNZ) and the New Zealand Financial Markets Authority (FMA).

Changes to the Credit Reporting Privacy Code (Amendment No. 14) were made in three stages in 2019, following a 18-month review into the operation of the comprehensive credit reporting system. These changes were intended to enhance the credit reporting system's fairness for consumers and improve enforcement and compliance.

Amendment No. 14 changes came into force on three phases on 1 July, 1 April, and 1 October 2019. The latest changes increased the threshold for listing overdue payments as defaults in credit reports. It also obliges credit providers to cease quotation inquiries when offering risk-based pricing for credit products.

Changes to the Superannuation Schemes Unique Identifier Code (Amendment No. 1) were made in three stages in 2019. The Code has been amended by Amendment No. 1 and commenced on 15 October 2015. Amendment No. 1 will make two minor changes to the Code. Firstly, it will amend the definition of the term "associated person" to replace a reference to section 587 of the Income Tax Act 1994 (which has since been repealed) with its current equivalent – paragraph 106 of the Income Tax Act 2007. Secondly, it will remove clause A2. This clause will not be extended or extended to new or existing entities and express prescribing in the Code but which are defined by the Privacy Act 1993 or Acts Interpretation Act 1901 which is the current equivalent to Acts Interpretation Act 1901. As at the date of this summary table, there is no concrete proposal for additional data privacy and protection rule.
The PDPA defines "personal data" as data relating to an identified or able to be identified natural person (a "data subject"), and includes any information that can be identified, whether true or not, from that information or from that information combined with other information or data. This information may reflect an identified individual's attributes or features, or any combination of such features, alone or when put together with other information.

The ASEAN Framework is designed to apply to all the ASEAN member states, and the Framework is intended to include all the personal data that is collected or otherwise processed by the ASEAN member states.

The Framework is intended to apply to information that would be subject to the Bill, whether the information is collected or held by an entity established in the country or from a person who undertakes an activity if:

- (1) A contract is entered into in the country; and
- (2) The personal data is intended to be processed within the country; and
- (3) An entity that has a branch or representative office in the country;

Philippines as long as it is processed within the Philippines.

The Bill is applicable to personal information and the personal data collected or otherwise processed in the Philippines, and the entity has a link with the Philippines, which includes the following:

- (a) The act, practice or activity is being done or practice engaged in in the country;
- (b) The entity has a link with the Philippines or even if the act, practice or activity is being done or practice engaged in outside the Philippines by an entity if:
- (1) The act, practice or activity relates to the information within the Philippines; and
- (2) The personal data is intended to be processed within the Philippines;
- (3) The personal data is intended to be processed within the Philippines, and
- (4) The personal data is intended to be processed within the Philippines, whether the personal data is intended to be processed within the Philippines or even if the act, practice or activity is being done or practice engaged in outside the Philippines.

The Bill is applicable to all the information that is collected or otherwise processed in the Philippines, and the entity has a link with the Philippines, which includes the following:

- (a) The act, practice or activity is being done or practice engaged in in the country;
- (b) The entity has a link with the Philippines; and
- (c) The personal data is intended to be processed within the Philippines.

In practice, this applies to any act, practice or activity that would be subject to the Bill, whether the information is collected or held by an entity established in the country or from a person who undertakes an activity if:

- (1) A contract is entered into in the country; and
- (2) The personal data is intended to be processed within the country; and
- (3) An entity that has a branch or representative office in the country;
<table>
<thead>
<tr>
<th>No.</th>
<th>Definition of 'sensitive' personal data (or similar) and (sensitive) personal data as defined by other legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU/UK</td>
<td>The EU/UK definitions of 'sensitive' personal data, as defined in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), include data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and sexual orientation.</td>
</tr>
<tr>
<td>China</td>
<td>The PRC Privacy Law defines sensitive personal data as a set of personal data that relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>India</td>
<td>The Indian Data Protection Bill, 2020 defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>The Hong Kong Personal Data (Privacy) Ordinance defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Singapore</td>
<td>The Singapore Personal Data Protection Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Malaysia</td>
<td>The Malaysia Personal Data Protection Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Thailand</td>
<td>The Thailand Personal Data Protection Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Indonesia</td>
<td>The Indonesia Personal Data Protection Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Japan</td>
<td>The Japanese Law on Personal Information Protection defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Vietnam</td>
<td>The Vietnamese Privacy Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Taiwan</td>
<td>The Taiwan Personal Information Protection Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
<tr>
<td>Australia</td>
<td>The Australian Privacy Act defines sensitive personal data as a set of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biological characteristics, health information, and sexual orientation.</td>
</tr>
</tbody>
</table>

**Sensitive information**

Sensitive information is personal information that includes information or an opinion about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, and sexual orientation. This information is generally accepted to be sensitive to state, and its collection, use, or disclosure requires special precautions.
<table>
<thead>
<tr>
<th>Sr.</th>
<th>EU/UK</th>
<th>APEC Privacy Framework and the ASEAN Framework</th>
<th>China</th>
<th>India</th>
<th>Hong Kong</th>
<th>Singapore</th>
<th>Malaysia</th>
<th>Thailand</th>
<th>Indonesia</th>
<th>Philippines</th>
<th>Vietnam</th>
<th>Japan</th>
<th>Taiwan</th>
<th>Australia</th>
<th>New Zealand</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>-</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>Important data is mentioned in the Data Cyber Security Law but the definition of important data has not yet been finalized, nor is there any indication as to how this will be enforced.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>Important data is not explicitly defined in the Cybersecurity Law. The definition of “critical personal data” (which the bill is concerned with) will be subject to future regulations.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>-</td>
<td>Important data is related to a number of sectors.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>11</td>
<td>-</td>
<td>The definition of “critical personal data” in Bill.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>12</td>
<td>-</td>
<td>The government will determine which data is critical to national security, defense, and economic stability.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>13</td>
<td>-</td>
<td>The Vietnamese government labels information as state secrets when:</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>14</td>
<td>-</td>
<td>- The information elates to a case, a circumstance, a location, a time, or a speech that contains important content in the fields of politics; national defense; national security; foreign affairs; economy; science; technology; or other subjects designated by the government.</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

None - critical data is not a defined concept under the GDPR.

N/A - Unclear definition

Important data is mentioned in the China Cyber Security Law but the definition of important data has not yet been finalized, nor is there any indication as to how this will be enforced. Important data includes data that is critical to national security, defense, and economic stability. The definition of “critical personal data” (which the bill is concerned with) will be subject to future regulations.

Payment data includes data that is critical to national security, defense, and economic stability. The definition of “critical personal data” (which the bill is concerned with) will be subject to future regulations.

The Indonesian government labels information as state secrets when:
- The information elates to a case, a circumstance, a location, a time, or a speech that contains important content in the fields of politics; national defense; national security; foreign affairs; economy; science; technology; or other subjects designated by the government.
- The disclosure of the information may cause harm to the State of the Republic of Vietnam.
Grounds for Collection, Processing and Transferring Data Processing

Under the China Cyber Security Law, an organisation shall establish a compliance strategy with a legal basis for personal data processing activities, and take necessary steps to ensure the protection of personal data processed. Consent is the legal basis for the collection, use or disclosure of personal data. For example, if required by a law, regulation or the provisions of an agreement, an organisation may collect the personal information, or if it is necessary:

- To achieve the lawful and reasonable purposes of data processing.
- To respond to a request from the data subject.
- To protect the data subject.
- For the controller to perform a contract to which the data subject is a party.
- To prevent or remedy violations of laws. There shall be no unconscionable contract to which the data subject is a party.
- For the controller to satisfy any legal obligation.
- To maintain the legitimate interests of the controller or third party.
- When collecting personal information, organisations and individuals must collect personal information only for the declared purposes, and not for any secondary purpose or other compatible purpose.
- If the purpose of data processing is to protect the data subject in accordance with the purpose for which the data is collected, the intended recipient of the data may disclose the personal information.

Furthermore, the agency obtaining data from any individual shall inform the data subject, the intended recipient of the information and the recipients of the consequences of the collection.

An approved information sharing agreement may authorize an agency to share any personal information that is not required to be collected for any public administration or law enforcement purpose.

Personal information shall not be collected by any person or agency, nor shall it be used for any purpose that is not specified by the data collection.

The collection, use and disclosure of personal information by any person or agency shall be in accordance with the terms of the agreement.

In particular, any person or agency that obtains personal information through collection, use and disclosure shall take necessary and reasonable measures to ensure the protection of personal information, including but not limited to:

- Implementing appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal information and any accidental loss, destruction or damage to personal information.
- Minimising the risks of processing personal information and ensuring that the personal information is available only to those persons who are necessary for the processing of the personal information.
- Ensuring that the personal information is processed in compliance with the terms of the agreement.
- Ensuring that the personal information is processed in a manner consistent with the terms of the agreement.

The individual shall have the right to withdraw consent at any time.

Agencies will not obtain personal information from any individual unless the individual consents to the collection of that information voluntarily.

The individual shall have the right to withdraw consent at any time.

If the purpose of data processing is to protect the data subject in accordance with the purpose for which the data is collected, the intended recipient of the data may disclose the personal information.

An approved information sharing agreement may authorize an agency to share any personal information that is not required to be collected for any public administration or law enforcement purpose.

Personal information shall not be collected by any person or agency, nor shall it be used for any purpose that is not specified by the data collection.

The collection, use and disclosure of personal information by any person or agency shall be in accordance with the terms of the agreement.

In particular, any person or agency that obtains personal information through collection, use and disclosure shall take necessary and reasonable measures to ensure the protection of personal information, including but not limited to:

- Implementing appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal information and any accidental loss, destruction or damage to personal information.
- Minimising the risks of processing personal information and ensuring that the personal information is available only to those persons who are necessary for the processing of the personal information.
- Ensuring that the personal information is processed in compliance with the terms of the agreement.
- Ensuring that the personal information is processed in a manner consistent with the terms of the agreement.

The individual shall have the right to withdraw consent at any time.

Agencies will not obtain personal information from any individual unless the individual consents to the collection of that information voluntarily.

The individual shall have the right to withdraw consent at any time.

If the purpose of data processing is to protect the data subject in accordance with the purpose for which the data is collected, the intended recipient of the data may disclose the personal information.

An approved information sharing agreement may authorize an agency to share any personal information that is not required to be collected for any public administration or law enforcement purpose.

Personal information shall not be collected by any person or agency, nor shall it be used for any purpose that is not specified by the data collection.

The collection, use and disclosure of personal information by any person or agency shall be in accordance with the terms of the agreement.

In particular, any person or agency that obtains personal information through collection, use and disclosure shall take necessary and reasonable measures to ensure the protection of personal information, including but not limited to:

- Implementing appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal information and any accidental loss, destruction or damage to personal information.
- Minimising the risks of processing personal information and ensuring that the personal information is available only to those persons who are necessary for the processing of the personal information.
- Ensuring that the personal information is processed in compliance with the terms of the agreement.
- Ensuring that the personal information is processed in a manner consistent with the terms of the agreement.

The individual shall have the right to withdraw consent at any time.

Agencies will not obtain personal information from any individual unless the individual consents to the collection of that information voluntarily.

The individual shall have the right to withdraw consent at any time.

If the purpose of data processing is to protect the data subject in accordance with the purpose for which the data is collected, the intended recipient of the data may disclose the personal information.
<table>
<thead>
<tr>
<th>EU / UK</th>
<th>APEC Privacy Framework and the ASEAN Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td></td>
</tr>
<tr>
<td>Thailand</td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td></td>
</tr>
<tr>
<td>Philippines</td>
<td></td>
</tr>
<tr>
<td>Vietnam</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td></td>
</tr>
</tbody>
</table>

• For the protection of lawful rights and interests of individuals.
  Consent to the processing of personal and sensitive information must be freely given, specific, informed, and evidenced by written, electronic or recorded means.

- or on behalf of, an enforcement body, or
  - the entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner.

Under the ASEAN Cyber Security Law, the rules of cross border data flows determine whether data transfer can be made to the third country. The new law stipulates that the PDPA will determine the adequacy of the third country.

Under all cross-border data transfers, the PDPA transfers the data to the 3rd country, which contravenes the PDPA’s requirement to ensure that personal data will be processed in a manner that is consistent with the protection of personal data as described in the PDPA.

A transferor should ensure that the foreign person or entity is a participant in a contractual arrangement, which provides comparable safeguards to those in the PDPA, or the transferor has reasonable grounds to believe that the foreign person or entity will provide similar protection for personal data.

A transfer of personal data must be made to a country or territory which is covered by a standard contractual clause or approved code of conduct, or where there are specific provisions in respect of that country or territory which are consistent with the requirements of the PDPA.

There are no specific requirements, or restrictions with which to comply in the process of this kind of data transfer.

Article 100 - Cross-Border Data Transfer

The PDPA requires that all personal data is handled in a manner that is consistent with the protection of personal data as described in the PDPA.

The PDPA will determine the adequacy of the third country.

Under the EU General Data Protection Regulation (GDPR), the rules of cross-border data transfers include the cross-border transfer of personal data, which is considered to be a supervisory data transfer.

Under the EU General Data Protection Regulation (GDPR), the rules of cross-border data transfers include the cross-border transfer of personal data, which is considered to be a supervisory data transfer.

Under Section 33 of the PDPA, the rules of cross-border data transfers include the cross-border transfer of personal data, which is considered to be a supervisory data transfer.

A transferor must ensure that the foreign person or entity is a participant in a contractual arrangement, which provides comparable safeguards to those in the PDPA, or the transferor has reasonable grounds to believe that the foreign person or entity will provide similar protection for personal data.

A transfer of personal data must be made to a country or territory which is covered by a standard contractual clause or approved code of conduct, or where there are specific provisions in respect of that country or territory which are consistent with the requirements of the PDPA.

There are no specific requirements, or restrictions with which to comply in the process of this kind of data transfer.
• Control of cross-border data flow activities
• Consider if any exceptions to Section 33 apply, including checking the White List published by the PDPC
• Maintain an inventory of personal data being transferred outside of Hong Kong
• Conduct regular audits and inspections on transfers' operations to ensure compliance with obligations under the data transfer agreement.

An example of such a binding scheme is the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System. Six of the 21 APEC economies participate in the system. We recommend inserting a definition of “country” into clause 15 to include a state, territory, province, or any other part of a country.

Criteria for prescribing binding schemes and countries
It is recommended inserting new clauses 212A and 212B to provide for the making of regulations prescribing countries and binding schemes for the purposes of IPP 12, and to set out the criteria that the Minister must consider before recommending that such regulations be made. The Minister would be able to prescribe that countries or binding schemes be prescribed if satisfied that personal information would be subject to comparable privacy safeguards overall, compared to those in the bill.
10. Subject to explicit consent of the data subject, or by the parties to the transaction, or by a law or other regulation applicable to the data subject or another person; or by the data subject; or by the parties to the transaction; or by any other means as set out in section 26 of the PDPA.

Critical Personal Data (the definition of which the DPA requires, shall only be processed and shared within India.

Processing of personal data is required to be shared in India.

(a) The public interest in that collection or, as the case requires, that disclosure outweighs the potential interference with the privacy of the individual that could result from that collection or, as the case requires, that disclosure.

(b) It is necessary for the performance of the data subject’s duties and functions; or for the purposes of national security, public safety, or the prevention or detection of crime.

(c) It is necessary for the prevention or detection of public health risks or the protection of health or the public interest in health.

(d) It is necessary for the protection of the data subject’s life or other personal or vital interests.

(e) The public interest in that collection or, as the case requires, that disclosure outweighs the potential interference with the privacy of the individual that could result from that collection or, as the case requires, that disclosure.

(f) The public interest in that collection or, as the case requires, that disclosure outweighs the potential interference with the privacy of the individual that could result from that collection or, as the case requires, that disclosure.

(g) It is necessary for the purposes of public administration or regulation.

(h) It is necessary for the purposes of scientific research or the purposes of statistical purposes.

(i) It is necessary for the purposes of legal claims or for the purposes of legal proceedings.

(j) It is necessary for the purposes of legal proceedings.

(k) It is necessary for the purposes of enforcement of laws.

(l) It is necessary for the purposes of the performance of laws.

(m) It is necessary for the purposes of the performance of laws.

(n) It is necessary for the purposes of the performance of laws.

(o) It is necessary for the purposes of the performance of laws.

(p) It is necessary for the purposes of the performance of laws.

(q) It is necessary for the purposes of the performance of laws.

(r) It is necessary for the purposes of the performance of laws.

(s) It is necessary for the purposes of the performance of laws.

(t) It is necessary for the purposes of the performance of laws.

(u) It is necessary for the purposes of the performance of laws.

(v) It is necessary for the purposes of the performance of laws.

(w) It is necessary for the purposes of the performance of laws.

(x) It is necessary for the purposes of the performance of laws.

(y) It is necessary for the purposes of the performance of laws.

(z) It is necessary for the purposes of the performance of laws.

AAPEX Privacy Framework and the ASEAN Framework

Critical Personal Data (the definition of which the DPA requires, shall only be processed and shared within India.

Processing of personal data is required to be shared in India.

(a) Consent is given by data subject.

(b) Consent is given by data subject.

(c) Consent is given by data subject.

(d) Consent is given by data subject.

(e) Consent is given by data subject.

(f) Consent is given by data subject.

(g) Consent is given by data subject.

(h) Consent is given by data subject.

(i) Consent is given by data subject.

(j) Consent is given by data subject.

(k) Consent is given by data subject.

(l) Consent is given by data subject.

(m) Consent is given by data subject.

(n) Consent is given by data subject.

(o) Consent is given by data subject.

(p) Consent is given by data subject.

(q) Consent is given by data subject.

(r) Consent is given by data subject.

(s) Consent is given by data subject.

(t) Consent is given by data subject.

(u) Consent is given by data subject.

(v) Consent is given by data subject.

(w) Consent is given by data subject.

(x) Consent is given by data subject.

(y) Consent is given by data subject.

(z) Consent is given by data subject.

AAPEX Privacy Framework and the ASEAN Framework

Critical Personal Data (the definition of which the DPA requires, shall only be processed and shared within India.

Processing of personal data is required to be shared in India.

(a) Consent is given by data subject.

(b) Consent is given by data subject.

(c) Consent is given by data subject.

(d) Consent is given by data subject.

(e) Consent is given by data subject.

(f) Consent is given by data subject.

(g) Consent is given by data subject.

(h) Consent is given by data subject.

(i) Consent is given by data subject.

(j) Consent is given by data subject.

(k) Consent is given by data subject.

(l) Consent is given by data subject.

(m) Consent is given by data subject.

(n) Consent is given by data subject.

(o) Consent is given by data subject.

(p) Consent is given by data subject.

(q) Consent is given by data subject.

(r) Consent is given by data subject.

(s) Consent is given by data subject.

(t) Consent is given by data subject.

(u) Consent is given by data subject.

(v) Consent is given by data subject.

(w) Consent is given by data subject.

(x) Consent is given by data subject.

(y) Consent is given by data subject.

(z) Consent is given by data subject.
11. Complexities and/or cross-processing or collection, D border, None EU / UK APEC Privacy

The implementation of the personal data protection principles is difficult in practice. We have not seen any real-world examples to date.

- GA 71 is currently being revised to implement the obligations required under GA 71.
- The implementation of the extraterritorial principles is difficult in practice. We have not seen any real-world examples to date.

The supplementary regulations issued under the PDPA (e.g., MAS 626, banks may be required to issue a notice ("Notice") to provide an undertaking to the SFC).

If the EDSP is a non-exclusively with an EDSP, the LC is required to issue a notice ("Notice") to provide an undertaking to the SFC.

The SFC’s powers regarding the breach of its statutory powers despite the circular. All LCs that use the Circular.

Unless the LC keeps its regulatory records and the obligations set out in GR 71 are recently seen any examples to date.

The supplementary regulations issued under the PDPA (e.g., MAS 626, banks may be required to issue a notice ("Notice") to provide an undertaking to the SFC).

The SFC’s powers regarding the breach of its statutory powers despite the circular. All LCs that use the Circular.

Unless the LC keeps its regulatory records and the obligations set out in GR 71 are recently seen any examples to date.

The supplementary regulations issued under the PDPA (e.g., MAS 626, banks may be required to issue a notice ("Notice") to provide an undertaking to the SFC).

The SFC’s powers regarding the breach of its statutory powers despite the circular. All LCs that use the Circular.

Unless the LC keeps its regulatory records and the obligations set out in GR 71 are recently seen any examples to date.