ASEAN Plus Group's Regional Regulatory Guide to Personal Data Protection in Asia-Pacific

August 2021

The Member Firms:

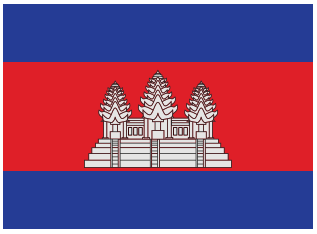
HOLDING REDLICH | RHTLaw Cambodia | 國浩律師事務所 GRANDALL LAW FIRM | F. ZIMMERN & CO. 施文律師行 | AMA | NASOETION & ATYANTO

PCA Law Paul Cheah Associates | VILLARAZA & ANGANGCO THE FIRM · EST. 1980 | RHTLaw Asia | DR A JU DAERYOOK & AJU | 理律法律事務所 LEE AND LI ATTORNEYS-AT-LAW | BGL | RHTLaw Vietnam International Capabilities Delivered Locally

ASEAN+ We know ASIA.

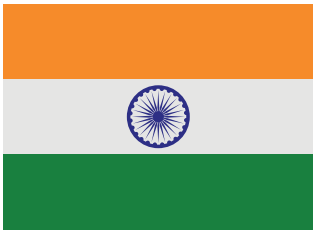
Content

03 Foreword



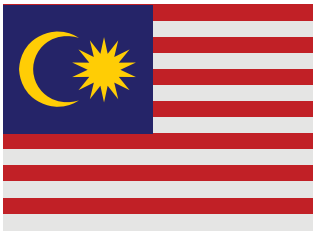
04 Cambodia
Vannak Houn
Liow Yee Kai
RHTLaw Cambodia

07 China
Henry Huang
Nicole Jiang
Grandall Law Firm



13 India
Anant Merathia
Poornima Devi
Anant Merathia & Associates

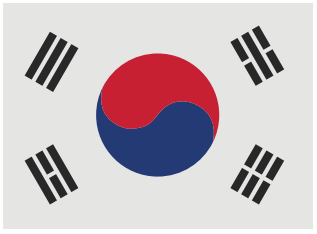
17 Indonesia
Genio Atyanto
Nasoetion & Atyanto



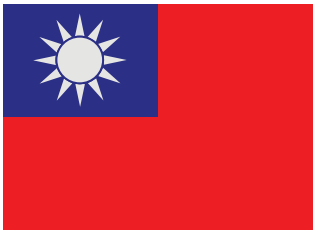
20 Malaysia
Mohanthas Narayanasamy
Paul Cheah Associates

24 Philippines
Franchette M. Acosta
Imperial, Paul Rodulfo B.
Villaraza & Angangco Law

30 Singapore
Piyush Gupta
R Saravanan
Wong Zhen
RHTLaw Asia LLP



35 South Korea
Timothy Dickens
DR & AJU LLC



38 Taiwan
Eddie Hsiung
Lee and Li

42 Thailand
Picharn Sukparangsee
Bangkok Global Law

48 Vietnam
Benjamin Yap
Mai Thi Ngoc Anh
RHTLaw Vietnam

Foreword

When the European Union published its General Data Protection Regulations (GDPR), it took the world by storm. People suddenly started taking ownership of their personal data and the rules regarding how such data was to be collected, processed, used and stored by companies, very seriously.

In Singapore, while the Republic's statute on personal data protection – the Personal Data Protection Act (PDPA) – had been in force since 2012, suffice to say, it came into prominence only after the GDPR had caught people's attention.

In fact, within ASEAN, Singapore has been one of the few countries that has had a law dedicated to protection of personal data of individuals for some time now. Some of the other countries within ASEAN have either not had a law specifically in relation to this (and are now scrambling to address this lacuna), or have introduced legislation to this effect very recently.

The ASEAN region is increasingly being viewed by international companies and conglomerates with a great deal of interest, but one of the block's stumbling points in attracting major investments has been the lack of a common set of rules / regulations in respect of protection of personal data of individuals.

This issue of the ASEAN Plus Group (APG)'s "Regulatory Guide to Personal Data Protection in Asia-Pacific" provides an overview of, and maps the key issues in some of the group's regional jurisdictions: Indonesia, Vietnam, Cambodia, Philippines, Malaysia, Thailand and Singapore. In addition, China, India, South Korea, and Taiwan (each significant economies with key relationships to ASEAN), are also represented in this Guide.

All country chapters are written by leading regulatory lawyers from their respective jurisdictions, providing valuable insights into their respective jurisdictions, supervisory regimes and key regulatory requirements.

We trust that you will find this Guide practical and helpful. The APG law firms listed in this Guide would be pleased to render their expert assistance to you in navigating the challenges and opportunities in the personal data protection space in this region to you.

Cambodia

Vannak Houn and Liow Yee Kai
RHTLaw Cambodia

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

As to date, Cambodia has not enacted any specific or comprehensive data protection law. The most recent legislation that contains provision for data protection is the E-Commerce Law which became effective in 2020. However, this law mainly covers the protection of data that are collected over the course of electronic records for the purpose of e-commerce activities in Cambodia.

The other legislations providing for protection of data can be found under the Right to Privacy provisions of the following:

(a) The Constitution of the Kingdom of Cambodia;

(b) The Civil Codes of Cambodia;

(c) The Criminal Codes of Cambodia;

(d) The E-Commerce Law;

(e) The Law on Telecommunication; and

(f) The Press Law.

Cambodia is a civil law system country which relies on the codification of written legal instruments and each legal instrument derives its validity and authority from the legal instrument placed above it in the hierarchical structure of laws. The hierarchy of law in Cambodia starts with the Constitution and all laws, legal instruments and governmental decisions must adhere to it.

Since there is no specific law governing data protection, in the event of a dispute in respect of data protection or any potential data protection breaches (in relation to the aforementioned legislations), the prevailing law should be the law that is applicable or relate to the matter of dispute. Where there is an issue over which law applies, the law that has higher hierarchy shall prevail.

Cambodia

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

There is no specific provision for extraterritorial jurisdiction and international data transfer under the above-mentioned legislations related to data protection. However, Article 32 of the newly enacted E-Commerce Law, which regulates domestic and cross-border e-commerce activities in Cambodia, states that any person who collects personal data or information for the purpose of e-commerce activities shall use all means to ensure that the provided personal data and private information are safely protected at all reasonable circumstances. As such, it is plausible that any personal data that has been collected either domestically or internationally through the online transaction for the purpose of e-commerce activities in Cambodia may subject to the jurisdiction of the E-Commerce Law.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

Subject to specific matter and the applicable law, each relevant authority is responsible for enforcing data protection in Cambodia. i.e. Article 23 and 49 of E-Commerce law give the authority to the Ministry of Commerce and the Ministry of Posts and Telecommunications to oversee and to enforce the implementation of the security procedures and electronic records for e-commerce activities in Cambodia. While the Criminal Code of Cambodia grants the law-enforcement and the court of the authority to enforce the protection of personal data over the violation of privacy.

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

Not Applicable.

5. What are penalties for non-compliance/violation with the data-protection laws in your jurisdiction country?

Any non-compliance or violation with the provision of data protection laws may lead to disciplinary sanctions, monetary penalties and imprisonment under each applicable law.

While each statute may ascribe a different monetary penalty, the same is usually in the range of about two million KHR to four million KHR (approximately USD 500 – 1,000) per incident, and a possible jail term ranging from one (1) month to two (2) years.

Cambodia

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

Although there is no specific standard procedure or forms that are required to be completed when submitting to the competence authority, Article 25 of the E-Commerce Law sets out responsibilities for the e-commerce service provider to take immediate actions and to notify the Ministry of Posts and Telecommunications in the event that such e-commerce service providers become aware that private information in the record might lead to civil and criminal proceedings. Those responsibilities are:

(a) To remove information from the system and stop providing services related to such information; and

(b) To store the information as evidence and notify the Ministry of Posts and Telecommunications and relevant competent ministries, institutions of the facts and identity of the suspects.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

Article 32 of E-Commerce Law stipulates the responsibility of the e-commerce service providers to take reasonable security measures to prevent the loss, access, use, modification, leakage, and the unauthorized disclosure of the data unless otherwise authorized by the information owners or by law.

8. Is there a minimum or maximum period for retaining personal data?

There is no minimum or maximum period of retention of personal data provided under the above-mentioned laws.

9. Are there any exceptions to the local data protection laws?

The Constitution of Cambodia and other applicable laws recognize the protection of personal data and the right to privacy, but there are exceptions that such protection might not apply to. For instance, the disclosure of personal data for the interest of public interest and safety.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

Although there is no single comprehensive, umbrella legislation governing the protection of data in Cambodia, the enforcement of data protection is arguably in place by the operation of other legislation and laws which provide, in a limited scope, for the protection of data. . With the new enactment of the E-Commerce Law, the Ministry of Commerce and the Ministry of Posts and Telecommunications are putting all of their efforts to enforce such protection. Many online businesses were asked to register their businesses with the ministry or risk being fined by the authorities.

In addition to the above, many initiatives have been proposed by the government for digital payment service providers to tighten their security measures including the protection of personal data.

China

Henry Huang and Nicole Jiang
Grandall Law Firm

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

The legislation work of data protection in China has been going through rapid development in recent years. With the promulgation of laws, regulations and guidelines, legal protection for data, including data security and personal information security, is becoming increasingly refined.

At the national level, there are three main acts constituting the legal framework of data protection in China, which is the *Cyber Security Law* ("**CSL"**), the *Data Security Law* ("**DSL**") and the *Personal Information Protection Law* (still soliciting public comments).

As the first law to address cybersecurity and data privacy protection, the CSL came into effect on June 1, 2017. After that, there have been numerous implementing regulations and guidelines proposed, released, or revised to elaborate the essentials and ideas introduced under the CSL. Such as the *Guidelines on Internet Personal Information Security Protection*, effective from April 19, 2019; the *National Standard of Information Security Technology – Personal Information Security Specification*, effective from May 1, 2018 of which the revised draft is currently circulated for consultation, etc.

In June 2021, the long-expected DSL was published after two versions of drafts and will come into force on September 1, 2021. The main purpose of DSL is to regulate data processing activities, safeguard data security, promote data development and utilization, protect the lawful rights and interests of individuals and organizations, and maintain national sovereignty, security and development interest. The concept of data classification, strengthening the governance of important data, strengthening the supervision of providing data stored in China to overseas judicial or law enforcement agencies, and the intensity of penalties are all highlights and focuses of the DSL. Therefore, different from the CSL of which the purpose is to protect cyber security, the DSL put more emphasis on the security of data itself. However, there is still some relevance and connection in between, which is, the tiered data security system of the DSL echoes with the multiple-level protection schemes of the CSL.

From the perspective of protection of personal information, attention shall be paid to the second draft of the *Personal Information Protection Law* ("**PIPL Draft**"), which is expected to be published in the near future. Compare with the above two laws, the PIPL Draft is more focused on individual rights in the personal information processing activities, such as the right of consent, denial, withdrawal, correction, deletion and report.

Apart from the CSL and relevant guidelines and regulations, the Civil Code, effective on January 1, 2021 also further reinforces the statutory right of privacy for individuals and establishes data protection principles. Applicability of other laws or regulations, such as the Criminal Law, E-Commerce Law, Consumer Rights Protection Law, will invariably depend on the factual context of each case.

At the provincial level, In June 2021, Shenzhen published the *Data Regulation of Shenzhen Special Economic Zone (Draft for Comments)*. This is the first law aimed at protecting personal data and regulating data processing activities by district government. However, how district law organically corresponds with the national statue still remain unclear and need to be tested in practice.

At present, the CSL and DSL are the main acts at the highest level regulating data security in China. Subject to the principle of application and hierarchy, the CSL and DSL shall prevail when facing data security dispute.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

■ Extraterritorial jurisdiction

The CSL provides limited extraterritorial application, whose extraterritorial effect applies only when any entity or person outside of China attacks, intrudes or otherwise causes damage to the critical information infrastructure and results in serious consequence.

Whilst, the DSL has a broader extraterritorial reach than that of the CSL, the DSL is applicable to all data processing activities conducted within the territory of the PRC and the supervision of their safety. However, should any data activities conducted by entities and persons outside of China impair the national security, public interest or the lawful rights and interests of any citizen or organization of the PRC, the DSL shall apply.

Besides, the PIPL Draft proposes more clear and specific extraterritorial application to overseas entities and individuals. Which is, if overseas entities and individuals process personal data of data subjects in China to provide products and/or services in China to data subjects, analyze or assess the behavior of data subjects in China or under other circumstances provided by Chinese laws and regulations, those activities shall be subject to the PIPL Draft.

■ International data transfer

Procedures for security assessment remain very unclear. The CSL imposes this requirement, but does not provide any guidelines, while other measures and regulations provide detailed guidelines on how to conduct a security assessment, but fails to be effective.

According to the CSL, if there is the need to share protected data with foreign entities, a security assessment should be conducted in accordance with the measures developed by the Cyber Administration of China (CAC) in conjunction with the relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation.

The *Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Draft for Comment)* issued by CAC in 2017 also provide further guidance on how the security assessment is to be carried out. Whether the relevant data may be transferred overseas would depend on the results of such security assessment. Later, in June 2019, CAC issued the *Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment)* ("**2019 Measures**"). Cross-border transfers of personal data by a network operator will be prohibited in certain circumstances under the 2019 Measures, including situations where the results of the security assessment indicate that the proposed cross-border transfer may impact China's national security, endanger public interest or the relevant network operator could not effectively protect personal information. However, whether and when these Measures will come into effect still remain unknown.

Also, the *PIPL Draft* addresses cross-border transfers of personal information if the data processor satisfies at least one of the following conditions prior to such transfer:

(i) Passed the security assessment organized by CAC;

(ii) Obtained a "personal information protection certification" conducted by a specialized organization in accordance with CAC provisions;

(iii) Entered into an agreement with the overseas recipient pursuant to CAC's requirements regarding the rights and obligations of both parties whereby the data processor shall monitor the recipient's compliance with the PIPL Draft; and/or

(iv) Complied with further requirements as set forth by the CAC.

However, data processor shall:

(i) Store personal information collected and generated in China within the territory of the PRC; and

(ii) Pass a prior security assessment with the CAC prior to any off-shore transmission thereof, in case a data processor either qualifies as "key information infrastructure operator" under the CSL, or handles personal information up to the volume threshold yet to be prescribed by the CAC.

In addition, the data processor shall have obtained the data subject's consent prior to the offshore transfer and have informed the data subject regarding:

(i) Overseas data processor's business identity/contact information

(ii) Purpose/method of data processing

(iii) Types of personal data processed

(iv) The data subject's rights against the overseas recipient

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

There is no single regulatory authority exclusively dealing with data protection matters. CAC is generally considered as the primary data protection authority in China, although various legislative and administrative authorities have claimed jurisdiction over data protection matters, such as the National People's Congress Standing Committee, the Ministry of Public Security, the Ministry of Industry and Information Technology, the State Administration for Market Regulation and the Ministry of Science and Technology.

Other sector-specific regulators, such as the People's Bank of China or the China Banking and Insurance Regulatory Commission, may also monitor and enforce data protection issues of regulated institutions within their respective sectors.

China

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

The CSL requires operator of a critical information infrastructure to designate a person in charge to fulfill the obligation of security protection. The DSL stipulates more clearly that, processors of important data are required to appoint a person in charge of data security to carry out the data security responsibilities. However, neither CSL or DSL specify whether such person in charge shall be defined as a DPO and no penalties is set for failing to do so.

Separately, the *National Standard of Information Security Technology – Personal Information Security Specification* ("**PISS**"), which was amended and effective from October 1, 2020 but not enforceable, requires an organization to appoint a data protection officer and a data protection department if the organization:

(a) Has more than 200 employees and its main business line involves data processing;

(b) Processes personal information of more than 1,000,000 individuals, or is estimated to process personal information of more than 1,000,000 individuals; or

(c) Processes sensitive personal information of more than 100,000 individuals.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

Various sanctions and penalties can apply, depending on the violation and the applicable regulation.

For non-compliance with data protection obligations, sanctions, and penalties usually include a warning, confiscation of illegal income, a fine of more than one time and less than ten times the illegal income and/or a fine depends on the actual situation. Under severe circumstances, suspension of the related business, suspension of the business for internal rectification, shutdown of the website, and revocation of related permits or licenses may be enforced.

Fine is the most common method among all punishment and penalties. Under the CSL, a fine can be charged from RMB 10,000 (approximately USD 1,600) to RMB 100,000 (approximately USD 16,000) to the management and other personnel who bear direct responsibility. Under the DSL, the amount of fine varies from RMB 50000 to RMB 10 million. However, the PIPL Draft increases the punishment significantly. Where serious circumstances arise, the data processor is subject to fines of up to RMB 50 million (approximately USD 7,830,000.00) or 5% of the turnover of the previous year.

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

The CSL introduced a general requirement for the reporting and notification of actual or suspected personal information breaches, which is, where personal information is leaked, lost or distorted (or if there is a potential for such incidents), organizations must promptly take relevant measures to mitigate any damage and notify the relevant data subjects and report to the relevant government agencies in a timely manner in accordance with relevant provisions. However, it neither defines data security breach, nor prescribes a standard process for reporting.

The DSL focuses a lot on security assessment and report. It requires that in carrying out data processing activities, risk monitoring shall be strengthened, and remedial measures shall be taken immediately when data security defects, loopholes

and other risks are found. In the event of a data security incident, immediate measures shall be taken, users shall be informed in a timely manner and report shall be made to relevant competent authorities. Important data processors shall, in accordance with relevant provisions, carry out regular risk assessments of their data processing activities and submit risk assessment reports to the relevant competent authorities. The risk assessment report shall include the type and quantity of important data to be processed, the situation of carrying out data processing activities, the data security risks faced and the corresponding measures, etc.

The PISS, together with other guiding circulars (such as the *National Network Security Incident Contingency Response Plan, the Guidelines for Internet Personal Information Security Protection*, etc.), provide some guidelines on the reporting and notification of personal information breaches or security incidents. For example, certain response and evaluative actions are required to be taken after the occurrence of a personal information security incident, such as taking a record of the substance of the incident, evaluating the possible impact of the incident, and adopting measures to control and eliminate risks. Nevertheless, these supplementary guidelines do not go further to provide a complete set of reporting procedures.

The PIPL Draft reinforced the mandatory data breach reporting requirement under the CSL. However, there is one exception that if the measures taken by the data processor could effectively avoid damages caused by disclosure of personal information, it is not necessary for the data processor to notify the data subjects unless the competent department considers otherwise.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

There are various of obligations on controllers/processors during the full cycle of data usage, such as obtaining consent, protection of users' rights and obligations, notification of breach, concluding qualified contract with third parties, conducting risk assessment, making records of handling situations, specifying ways of withdrawing, deleting or revising personal information.

8. Is there a minimum or maximum period for retaining personal data?

PIPL Draft requires a 3-year retention of personal information in the following circumstances:

(a) Handling sensitive personal information;

(b) Using of personal information for automated decision-making;

(c) Entrusting the handling of personal information, providing personal information to others, or disclosing personal information;

(d) Providing personal information abroad; and/or

(e) Other personal information handling activities that have a major impact on individuals.

China 

9. Are there any exceptions to the local data protection laws?

In general, express consent, the primary basis for lawful usage of personal data, is required from the data subject before personal information is collected, used, transferred or otherwise processed. However, there are some exceptional circumstance under the PIPL Draft in which personal information can be processed without consent, including:

(a) Entering into or fulfilling a contract where the data subject is a named party;

(b) Fulfilling legal obligations;

(c) In response to public health incidents;

(d) For public security and public interest reasons; or

(e) As required by another PRC law.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

The enforcement environment is evolving rapidly as the whole society is increasingly becoming aware of individual's data protection rights. Therefore, the tendency is that laws and regulations are intended to enhance the regulators' powers of enforcement and increase the amount of fines for violation, which can be told from the answer to question 5.

Meanwhile, another trend is that the enforcement of date protection laws is welcoming continuous refinement in specific industries and sectors. For example, the CAC published the *Rules on the Administration of Automobile Data Security (Draft for Comments)* in May, which aims at regulating automobile data processing activities specifically.

India

Anant Merathia and Poornima Devi
Anant Merathia & Associates

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

India has not yet enacted specific legislation on data protection. However, the *Information Technology Act, 2000* ("**IT Act**") and *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* ("**SPDI Rules**") do cater to some aspects of data protection, albeit at a minuscule level. Amendments were made to the IT Act in the year 2009 which give a right to compensation for improper disclosure of personal information.

Also, some provisions of the *Aadhaar (Targeted Delivery of Financial and Other Subsidies Act) 2016* deal with the personal information and its protection.

In addition to the above, the following draft laws and policies that regulate data protection principles are at various stages of discussion:

(a) *Personal Data Protection Bill, 2019* ("**PDP Bill**"), which is currently pending before the Lok Sabha (i.e., the Lower House or House of the People) of the Parliament of India;

(b) *Non-Personal Data Governance Framework* (the "**NPD Framework**"), which is *currently* being deliberated by the Committee of Experts constituted under the Ministry of Electronics and Information Technology (the "**MeitY**");

(c) *Digital Information Security in Healthcare Act, 2017* ("**DISHA**"); and

(d) *National Digital Health Mission* (the "**NDHM**") and *Health Data Management Policy* issued by the Ministry of Health and Family Welfare.

Some of these draft laws will replace or modify existing laws once they are enacted and come into force. In particular, the PDP Bill is a much debated and deliberated draft law that aims to introduce similar provisions as the GDPR into data protection law in India.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

Rule 7 of the SPDI Rules allows the cross-border transfer of sensitive personal data by body corporate to those countries that ensures the same level of data protection that is expected under the IT Act and SDPI Rules. Cross border transfer is only allowed in 2 cases:

(a) Performance of a lawful contract between the body corporate and the person whose data has been transferred; or

(b) If the person has consented to the data transfer.

There is no restriction under the SPDI Rules regarding cross-border dataflows of information that is not sensitive personal data or information.

The PDP Bill proposes a new regime for cross-border transfer of personal data. Upon introduction, there would seemingly be separate requirements for sensitive personal data and critical personal data. Sensitive personal data could be transferred outside India only with the express consent of the individual and in compliance with standard contractual clauses or intra group schemes approved by the Authority formed under the said legislation. Critical personal data could be transferred only to a person or entity providing emergency health services if such transfer is necessary for prompt action. The Central Government would define what constitutes critical personal data.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

India does not have a national regulatory authority for protection of personal data.

The Ministry of Electronics & Information Technology (Government of India), Department of Electronics and Information Technology (i.e., MeitY) is responsible for administering the IT Act and issuing the rules and other clarifications under the IT Act. The authorities established under the IT Act – i.e. the adjudicating officer and cyber appellate tribunal and, thereafter, the different High Courts and the Supreme Court, are responsible for enforcing the IT Act.

The PDP Bill proposes creating a Data Protection Authority of India (the "**Authority**"). The Authority, when established and created will be responsible for protecting the interests of data principals, preventing misuse of personal data and ensuring compliance with the new law.

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

Under the SPDI Rules, body corporates are required to designate a grievance officer and there is no general requirement to appoint a Data Protection Officer.

The PDP Bill proposes that a data fiduciary classified as significant as per the norms laid down in the Bill, must appoint a data protection officer.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

Compensation for failure to protect data (Section 43A of the IT Act) – Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate *shall be liable to pay damages by way of compensation to the person so affected.*

The PDP Bill proposes that data principals who have suffered harm as a result of any violation of the requirements of the PDP Bill can seek compensation from the data fiduciary or the data processor. (i.e., *tentative Section 64 of the PDP Bill*)

Punishment for disclosure of information in breach of lawful contract (Section 72A of the IT Act) – Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing

personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three (3) years, or with fine which may extend to five lakh rupees (approximately USD 7,000), or with both.

The PDP Bill proposes penalties linked to worldwide turnover. Those penalties can range from 2% or 4% of the worldwide turnover, depending on the type of breach. (i.e., *tentative Section 57 of the PDP Bill*).

Penalty for Breach of confidentiality and privacy (Section 72 of the IT Act) – If any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two (2) years, or with fine which may extend to one lakh rupees (approximately USD 1,400), or with both.

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

There is no specific provision or mandatory standard process or form to be followed whilst reporting data breaches.

However, the PDP Bill does contain provisions dealing with the process of reporting personal data breach (i.e., *tentative Section 25*). The PDP Bill envisages that a data fiduciary would have to inform the Data Protection Authority of India by way of a notice which would have to contain the following particulars (i.e., *tentative Section 25(2) of the PDP Bill*):

(a) Nature of personal data which is the subject-matter of the breach;

(b) Number of data principals affected by the breach;

(c) Possible consequences of the breach; and

(d) Action being taken by the data fiduciary to remedy the breach.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

Indian law does not contain the concepts of controller and processor. The SPDI Rules do not contemplate the concepts of, or distinguish between controllers and processors. Instead, the SPDI Rules refer to the concept of a 'body corporate' and a 'provider of information'. A body corporate is defined as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities". The 'provider of information' is the natural person who provide sensitive personal data or information to a body corporate.

A body corporate is required to have its security practice and procedures certified and audited by an independent auditor who is approved by the central government at least once every year, or when there is a significant upgrade in its computer resource.

The PDP Bill proposes the concepts of a 'data fiduciary' and a 'data processor'. A 'data fiduciary' and a 'data processor' are equivalent to the concept of controller and processor under the GDPR. The PDP Bill proposes that both the data fiduciary and data processor have to implement appropriate security safeguards.

India 

8. Is there a minimum or maximum period for retaining personal data?

Section 67C of the IT Act requires that an intermediary preserve and retain information in a manner and format and for such period of time as prescribed by the central government.

The PDP Bill states that a data fiduciary may not retain personal data beyond the period necessary to satisfy the purpose for which it is processed (i.e., *tentative Section 9 of the PDP Bill*). It also states that such data must be deleted at the end of this period. However, the Bill also allows for longer periods of retention if required by compliance with legal obligations, or if the consent of the data principal has been obtained, and prescribes periodic reviews by data fiduciaries for an ongoing assessment of the continued necessity of the retention of personal data.

9. Are there any exceptions to the local data protection laws?

The PDP Bill envisages exemption of certain provisions for certain processing of personal data in the following scenarios (i.e., *tentative Section 36 of the PDP Bill*).

(a) Personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force;

(b) Disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding;

(c) Processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;

(d) Personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or

(e) Processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

Personal data is protected through indirect safeguards developed by the courts under common law, principles of equity and the law of breach of confidence. In a landmark judgment delivered in August 2017 (i.e., *Justice K.S Puttaswami & another Vs. Union of India*), the Supreme Court of India has recognised the right to privacy as a fundamental right under Article 21 of the Constitution of India as a part of the right to "life" and "personal liberty". This landmark treatise on the subject of privacy explicitly overrules previous judgements of the Supreme Court which had held that there is no fundamental right to privacy under the Indian Constitution.

"*Informational privacy*" has been recognised as being a facet of the right to privacy and the court held that information about a person and the right to access that information also needs to be given the protection of privacy.

In the post-*Puttaswamy* landscape, varying stances have been adopted by different high courts in different states, and it is safe to assume that until the PDP Bill comes into effect, the scope and impact of these rights will continue to be judicially debated.

Indonesia

Genio Atyanto
Nasoetion & Atyanto

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

Fundamentally, the protection of personal data is regulated in Article 28 G paragraph (1) of the 1945 Constitution, which states that "Any person has the right to protection of himself, family, honor, dignity, and property under his control, and the right to a sense of security and protection from the threat of fear to do or not do something that is a human right".

In addition to the above, there is no specific law on personal data protection in Indonesia as the implementation. Currently, the Indonesian government is drafting a personal data protection bill ("**Data Privacy Bill**") that will serve as the umbrella for regulating personal data protection in Indonesia. However, several laws and regulations provide protections on the personal data used in the electronic system.

Indonesia has enacted Law No. 11 Year 2008 on Electronic Information and Transactions as amended by Law No. 19 Year 2016 ("**ITE Law**") that was expected to provide legal certainty on the use of information technology and electronic transactions in Indonesia, including the principle of the use of electronic information of a party that must be based on the consent of the information owner. To further implement the ITE Law specifically on the provision regarding the protection of the personal data on the electronic system, the Minister of Communications and Information (the "**MCI**") has issued a Regulation No. 20 Year 2016 on Protection of Personal Data in Electronic Systems ("**MCI Reg 20/2016**").

Other than the ITE Law and MCI Reg 20/2016, there are also other regulations that have personal data protection elements, such as:

(a) Law No. 7 Year 1992 on the Banking as lastly amended by Law No. 11 Year 2020;

(b) Law No. 8 Year 1999 on the Consumer Protection;

(c) Law No. 36 Year 1999 on the Telecommunications;

(d) Law No. 23 Year 2006 on the Resident Administration as amended by Law No. 24 Year 2013;

(e) Law No. 14 Year 2008 on the Transparency of Public Information;

(f) Law No. 36 Year 2009 on the Health as lastly amended by Law No. 11 Year 2020;

(g) Government Regulation No. 71 Year 2019 on the Organization of Electronic Systems and Transactions; and

(h) MCI Regulation No. 4 Year 2016 on the Information Security Management System, as well as other sectoral regulations.

If there is a conflict between the above regulations relating to personal data protection, the most relevant regulation to the disputed matter shall prevail.

Indonesia

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

ITE Law applies to any person who commits legal actions under the ITE Law, both in Indonesia and outside the territory of Indonesia, which has legal consequences in the Indonesian jurisdiction and/or outside the jurisdiction of Indonesia, and is detrimental to Indonesia's interests.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

MCI has a duty to carry out supervision for the implementation of MCI Reg 20/2016, either directly or indirectly. In this case, MCI has the authority to request data and information from electronic system providers in the context of protecting the personal data. MCI delegates this authority to the Director General in the field of informatics applications. The Director General is also tasked with providing education to the public regarding personal data. In addition, the role of sectoral supervisors is also significant for the implementation of personal data protection. For example, in the financial services sector, supervision is carried out by the Financial Services Authority (*Otoritas Jasa Keuangan*).

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

In Indonesia, there is no obligation to appoint a data protection officer. However, in the Data Privacy Bill there is a clause that, in certain circumstances, personal data controllers and personal data processors are required to appoint an official or officer who carries out the personal data protection function. Specific responsibility is ascribed which includes, among others:

(a) Processing of personal data for the benefit of public services;

(b) The core business of the personal data controllers requires regular and large-scale monitoring; and

(c) The core business of the personal data controllers consists of large-scale processing of personal data for specific personal data and/or related to criminal acts.

So far, based on Article 29 (i) MCI Reg 20/2016, the electronic system operator only has the obligation to provide a contact person who can be contacted by the owner of personal data regarding the management of their personal data.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

The penalties vary depending on the type of violation. For example, penalties can be in the form of oral and/or written warnings, temporary suspension of activities, announcements on online sites, fines, and imprisonment. The following non-compliance and/or violations may attract, depending on the violation set out below, imprisonment up to ten (10) years and/or a maximum fine of IDR 5 billion (approximately USD 70,000):

(a) Intentionally and without rights or unlawfully accesses a computer and/or electronic system belonging to another person;

(b) Interception or wiretapping of electronic information and/or electronic documents;

Indonesia

(c) Modifying, adding, reducing, transmitting, destroying, removing, transferring, hiding an electronic information and/or electronic document belonging to another person or belonging to the public and make it accessible to the public with improper data integrity; or

(d) Transferring or moving electronic information and/or electronic documents to other unauthorized electronic systems.

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

According to Article 28 (c) MCI Reg 20/2016, the electronic system provider has an obligation to only notify to the owner of personal data if there is a failure of protection in their electronic system.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

There is no current provision regulating controllers/processors in Indonesia today. However, it has been stipulated on the Data Privacy Bill.

8. Is there a minimum or maximum period for retaining personal data?

Article 15 paragraph (3) MCI Reg 20/2016 mandates the period for storing personal data in an electronic system according to the provisions of each supervisor's laws and regulations. However, if there are no provisions in the laws and regulations that specifically regulate it, it must be kept for at least five (5) years.

9. Are there any exceptions to the local data protection laws?

In general, there is no exception, except in instances where personal data is disclosed for the purposes of law enforcement at the request of the police, prosecutors, or other institutions whose authority is determined based on the applicable law.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

In 2020, there was a massive data leak in Indonesia by a unicorn company in the e-commerce field. The leak reached 91 million user data, including their full name, telephone number and personal email. Various parties stated that the company's failure to implement personal data protection was due to weak regulations in Indonesia covering personal data protection and cyber-crime. The judge ruled that the court was not authorized to examine the case. The court has not examined the merit of the case. To the best of our knowledge, there is no high-profile case in relation to the breach of personal data protection regulations. The party whose personal data has been illegally breached may be reluctant to bring the case to the court due to the absence of law that provide legal certainty on the enforcement of the regulations.

Malaysia

Mohanthas Narayanasamy
Paul Cheah Associates

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

The Personal Data Protection Act 2010 ("**PDPA**") is the primary legislation governing data protection and data privacy in Malaysia which came into force in Malaysia on 15th November 2013. Its main objective is to protect the personal data of users in respect of commercial transactions from the point the data is collected, used, stored, and destroyed.

(a) Subsidiary legislation pursuant to the PDPA that has been passed to date includes:

(b) Personal Data Protection Regulations 2013;

(c) Personal Data Protection (Class of Data Users) Order 2013;

(d) Personal Data Protection (Registration of Data User) Regulations 2013;

(e) Personal Data Protection (Fees) Regulations 2013;

(f) Personal Data Protection (Compounding of Offences) Regulations 2016; and

(g) Personal Data Protection (Class of Data Users) (Amendment) Order 2016.

Bank Negara Malaysia (BNM)

BNM has issued several guidelines and policy documents which address the obligation of financial institutions in respect of management of customer information. BNM has published a Privacy Statement which is applicable to personal data collected by the Bank, but excludes the following:

(a) Personal data collected by other entities including those owned or controlled by or affiliated to the Bank;

(b) Individuals who are not employees or agents of the Bank; or

(c) Any websites not under the control of the Bank.

Other legislation which governs various offences in relation to content in the form of data are:

(a) Computer Crimes Act 1997;

(b) Communication and Multimedia Act 1998 ("**CMA**");

(c) Digital Signature Act 1997;

(d) Electronic Commerce Act 2006;

(e) Electronic Government Activities Act 2007;

(f) Consumer Protection Act 1999;

(g) Official Secrets Act 1972;

(h) Sedition Act 1948;

(i) Sexual Offences Against Children Act 2017; and

(j) Penal Code – which governs criminal offences e.g online scams, cheating by impersonation etc.

With respect to conflict of laws, section 233(1)(a) of the CMA which governs content published over a network had issues of constitutionality i.e whether section 233 is inconsistent with Articles 5(1), 8 and 10 of the Federal Constitution.

Apart for the above, there has not been any overlap of regulatory jurisdiction primarily as each breach or crime relating to some form of data have sufficient peculiarity to fit the specific applicable laws.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

Personal data may not be transferred by the data user outside of Malaysia unless the transfer is to a country with sufficient data protection laws, as specified by the Minister in a Government Gazette.

However, personal data may be transferred abroad in the following circumstances:

(a) Consent has been given by the data subject for the transfer;

(b) The transfer is necessary for the performance of a contract between the data subject and data user;

(c) The transfer is necessary to perform or conclude a contract between the data user and third party;

(d) The transfer is for legal proceedings or obtaining legal advice or for establishing, exercising or defending legal rights;

(e) The data user has reasonable grounds for doing so;

(f) The data user has taken reasonable precautions to ensure the personal data will not be processed in any manner which contravenes the PDPA; or

(g) The transfer is necessary to protect the data subject's vital interests.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

(a) The Personal Data Protection Department (PDPD) oversees the processing of personal data of individuals involved in commercial transactions by the data user and to ensure that personal data collected is not misused and misapplied by the data user and/or the data processor unless it is for authorized purposes with the consent of the data subject. A data user processes personal data or has control over the processing of the personal data. This processing must be done for authorized purposes with the consent of the data subject. Any misuse of the data will make the data user liable under the act.

(b) The Personal Data Protection Commissioner is responsible for administering and enforcing the PDPA (and also the Digital Signature Act) and to:

(i) Implement and enforce personal data protection laws including the formulation of operational policies and procedures;

(ii) Conduct investigations where complaints are made to the PDPC;

(iii) Issue circulars, enforcement notices or any other instruments.

Prosecution for an offence can be instituted with the written consent of the Public Prosecutor. The Sessions Courts has the jurisdiction to try offences under PDPA.

(c) The Royal Malaysia Police (RMP) – Commercial Crime Investigation Department; investigates and Public Prosecutor prosecutes criminal offences eg Computer Crimes Act 1997, Penal Code etc.

(d) The Malaysian Communications and Multimedia Commission (MCMC) – investigates and prosecutes under the Communications and Multimedia Act 1998 which covers communications over the electronic media and prosecutes offences under the Digital Signature Act;

(e) The National Cyber Security Agency (NACSA) – Oversees all national cyber security functions formed under the National Security Council of Malaysia; and

(f) The Malaysia Computer Emergency Response Team (MyCERT) – Deals with computer security incidents such as intrusion, identity theft, malware infection, cyber harassment etc.

4. Is the appointment of a Data Protection Officer ("DPO") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

As of to-date, the law in Malaysia does not mandate the appointment of a Data Protection Officer. In normal circumstances, a compliance officer in an organization will be in charge of the matters in relation to personal data protection. Notwithstanding, the Ministry of Communications and Multimedia Malaysia is considering introducing an obligation in the PDPA, for a data user to appoint a DPO and to introduce a guideline in respect of such appointment.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

(a) Non-compliance of the PDPA may lead to a penalty between RM100,000 (approximately USD 24,000) to RM500,000 (approximately USD 121,000) and/or between one (1) to three (3) years of imprisonment;

(b) Non-compliance of the CMA – On conviction shall be liable to a fine not exceeding RM50,000 (approximately USD 12,000) or to imprisonment for a term not exceeding one (1) year or both;

(c) Computer Crimes Act 97 – On conviction shall be liable to a fine not exceeding RM50,000 (approximately USD 12,000) or to imprisonment for a term not exceeding five (5) years or to both;

(d) Official Secrets Act 1972 – On conviction punishable to imprisonment for a term not less than one (1) year but not exceeding seven (7) years.

Malaysia

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

There is no provision in the PDPA instructing a Data User to report any incident of a data breach to the authority.

Having said that, however, the PDP Commissioner is considering the addition of a new provision in the PDPA to mandate the report of a data breach incident by the Data User.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

The PDPA contains specific provisions for data processor. However, a Data Processor that processes personal data solely on behalf of a Data User may not be bound directly by the provisions of the PDPA, it is the duty of the Data User instead to ensure compliance by the Data Processor with the relevant provisions under the PDPA.

8. Is there a minimum or maximum period for retaining personal data?

The PDPA does not specify the period for the personal data to be retained. It may be retained by a Data User so long as it is necessary to fulfil the purpose for which it was collected and in regard to the Data User's business needs.

In the event a Data User requires the personal data to be retained beyond a specified statutory period, reasonable reasons to retain the personal data must be shown.

9. Are there any exceptions to the local data protection laws?

Yes. There are certain exceptions in the PDPA. These exceptions are set out below:

(a) Personal data processed outside Malaysia unless the data is intended to be further processed in Malaysia.

(b) A data user who is not established in Malaysia, unless that person uses equipment in Malaysia to process personal data, other than for the purpose of transit through Malaysia.

(c) The Government of Malaysia and state governments.

(d) Any information processed for the purposes of a credit reporting business under the Credit Reporting Agencies Act 2010.

(e) Data collected/processed for the prevention and/or detection of crime for the purpose of preparing statistics and/or research in accordance with a court order and/or for the purpose of discharging regulatory functions.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

There have been a number of instances of data breaches under the Malaysian PDPA in the last few years, however, details of the outcome of these cases are not clear. Till date, the regulation has not imposed any monetary and/or other penalties for such data breaches. The trend is clear that much commitment is needed for vigorous enforcement of data breaches and publicity of its outcome under the PDPA. However, it is hoped that the Public Consultation Paper No. 01/2020 (PC01/2020) referred to above has many initiatives for proposed amendments to the PDPA which is anticipated in the near future.

Philippines

Franchette M. Acosta and Imperial, Paul Rodulfo B.
Villaraza & Angangco Law

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

The Data Privacy Act of 2012 ("**DPA**") is the primary legislation governing data protection in the Philippines. The DPA applies to the processing of all types of personal data by any natural or juridical person if:

(a) The person involved in said processing is found or established in the Philippines;

(b) The processing relates to personal data about a Philippine citizen or resident;

(c) The processing is being done in the Philippines; or

(d) The processing is done or engaged in by an entity with links to the Philippines, with due consideration to international law and comity, such as but not limited to:

  (i) Use of equipment located in the country or maintenance of an office, branch, or agency in the Philippines for processing of personal data;

  (ii) Contracts entered into in the Philippines;

  (iii) A juridical entity unincorporated in the Philippines but has central management and control in the Philippines;

  (iv) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal data;

  (v) An entity that carries on business in the Philippines; and

  (vi) An entity that collects or holds personal data in the Philippines.

In addition to the DPA, the following are laws with provisions relating to data protection:

(a) The **Cybercrime Prevention Act of 2012** (Republic Act No. 10175), which prohibits, among others:

  (i) Offenses against the confidentiality, integrity and availability of computer data, including illegal access, illegal interception, data interference, system inference and misuse of devices; and

  (ii) Computer-related offenses, such as computer-related forgery, computer-related fraud and computer-related identity theft;

(c) The **Electronic Commerce Act of 2000** (Republic Act No. 8792), which applies to any kind of data message and electronic document used in the context of commercial and non-commercial activities, including domestic and international dealings, transactions, arrangements, agreements contracts and exchanges and storage of information;

(d) The **Access Devices Regulation Act of 1998** (Republic Act No. 8484), which prohibits access device fraud, including disclosing any information imprinted on the access device, such as, but not limited to, the account number or name or address of the device holder, without the latter's authority or permission.

A canon of statutory construction in the Philippines is that special laws prevail over general laws. Thus, in the event that the DPA and a more specific statute both apply and are in conflict, the latter shall prevail unless the same provides otherwise.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

Yes, the DPA may have extraterritorial application and cover international data transfers. As discussed above, even if the person undertaking the processing is not found or established in the Philippines or the processing is not undertaken in the Philippines, the DPA may apply if the processing relates to personal data about a Philippine citizen or resident or the processing is done or engaged in by an entity with links to the Philippines.

Further, the DPA provides that a personal information controller (PIC) shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a personal information processor (PIP) or a third party for processing, whether domestically or internationally.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

The regulatory authority responsible for the administration and enforcement of the DPA is the National Privacy Commission (NPC).

The NPC has issued implementing rules and regulations for the DPA ("**DPA IRR**") to provide the necessary particulars for the enforcement of the DPA. It has likewise issued circulars and advisories, compliance with which is mandatory, as well as advisory opinions which, though not binding, are instructive as to the NPC's standards in implementing the DPA.

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

The appointment of a DPO (as part of the registration of data processing systems) is required when:

(a) The PIC or PIP employs at least 250 persons;

(b) The processing carried out by the PIC or PIP is likely to pose a risk to the rights and freedoms of data subjects;

(c) Such processing is not occasional; or

(d) The processing includes the sensitive personal information of at least 1,000 individuals.

Philippines

The NPC recently released the draft *Guidelines on Administrative Fines* for specific violations of the DPA other than those listed in the DPA IRR. While the same is in the process of being finalized, we note that for failure to implement reasonable and appropriate measures to protect personal information, which include organizational security measures, it imposes a fine amounting to 1-5% of an entity's annual gross income. Further, failure to register true and updated information as regards data processing systems (of which the appointment of a DPO is part) may be subject to a fine not less than PhP 50,000.00 (approximately USD 1050) but not exceeding PhP 100,000.00 (approximately USD 2100).

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

Under the DPA IRR, the following violations of the DPA may result in imprisonment with a sentence ranging from one (1) to six (6) years, and a possible fine of PHP 100,000 (approximately USD 2100) to PHP 2,000,000 (approximately USD 42,000):

(a) Unauthorized processing of personal information;

(b) Unauthorized processing of sensitive personal information;

(c) Accessing personal information due to negligence;

(d) Accessing sensitive personal information due to negligence;

(e) Improper disposal of personal information;

(f) Improper disposal of sensitive personal information;

(g) Unauthorized processing of personal information;

(h) Unauthorized processing of sensitive personal information;

(i) Unauthorized access or intentional breach;

(j) Concealment of security breaches involving sensitive personal information;

(k) Malicious disclosure;

(l) Unauthorized disclosure of personal information; and

(m) Unauthorized disclosure of sensitive personal information.

In the event that a violation consists of a combination or series of acts from 5(a) to (m) above, the violators will be punished with an imprisonment term which may extend to six (6) years, but no less than three (3) years, and a fine amounting to PHP 1,000,000 (approximately USD 21,000) to PHP 5,000,000 (approximately USD 105,000.00).

The maximum penalty shall be imposed when the personal data of at least 100 persons are harmed, affected, or involved as a result of any of the above-mentioned offenses. Where the offender is a corporation, partnership or other juridical person, the penalty shall be imposed upon the responsible officers who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is an alien, in addition to the above penalties, the offender may be deported without further proceedings after serving the penalties. If the offender is a public official or employee, in addition to the above penalties, the person shall suffer perpetual or temporary absolute disqualification from office.

The NPC has likewise issued draft *Guidelines on Administrative Fines* for other specific violations of the DPA. The same has not yet been officially adopted.

Philippines

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

Notification to the NPC of a data breach is required when:

(a) The personal data involves sensitive personal information or any other information that may be used to enable identity fraud;

(b) There is reason to believe that the information may have been acquired by an unauthorized person; and

(c) The PIC or the NPC believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Notification to the NPC must be made within 72 hours upon knowledge of or the reasonable belief by the PIC or PIP that a personal data breach has occurred. Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

However, there shall be no delay in the notification if the breach involves at least 100 data subjects, or the disclosure of sensitive personal information will harm or adversely affect a data subject. In both instances, the NPC shall be notified within the aforementioned 72-hour period based on available information. The full report of the personal data breach must be thereafter submitted within five (5) days, unless the personal information controller is granted additional time by the NPC to comply.

Notification shall be in the form of a report, with the name and contact details of the DPO and the designated representative of the PIC indicated, and contain information on:

(i) The nature of the breach;

(ii) The personal data possibly involved; and

(iii) Measures taken to address the breach.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

Generally, PICs and PIPs are required to implement reasonable and appropriate organizational, physical and technical security measures for the protection of personal data. The data privacy principles of transparency, legitimate purpose and proportionality must likewise be abided by in the processing and protection of personal data.

8. Is there a minimum or maximum period for retaining personal data?

There is no set period provided for in the DPA or DPA IRR. The DPA simply provides that retention of personal data shall only be for as long as necessary:

(a) For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;

(b) For the establishment, exercise or defense of legal claims; or

(c) For legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, when provided by law, may be stored for longer periods, subject to implementation of the appropriate security measures. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

However, personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

9. Are there any exceptions to the local data protection laws?

Yes. Under the DPA, the DPA shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

(a) Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to:

  (i) Information about any individual who is or was an officer or employee of government that related to his or her positions or functions;

  (ii) Information about an individual who is or was performing a service under contract for a government institution, but only in so far as it relates to such service, including the name of the individual and the terms of his or her contract; and

  (iii) Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature of the benefit, provided that they do not include benefits given in the course of an ordinary transaction or as a matter of right.

(b) Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;

(c) Personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;

(d) Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law;

(e) Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or *Bangko Sentral ng Pilipinas*, and other bodies authorized by law, to the extent necessary to comply with applicable laws;

(f) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption.

Philippines 

10. What have been the enforcement trends for data protection laws in your jurisdiction?

As the DPA is fairly new legislation in the Philippines, there is no jurisprudence on the matter. The NPC, however, has been increasing its efforts to ensure that the DPA is complied with, particularly in light of the increase in online activities as a result of shelter-in-place measures and the amount of data processing involved in COVID-19 prevention measures such as contact tracing. The NPC recently released *Guidelines on the Processing of Personal Data for Loan-Related Transactions*, *Guidelines on the Use of Telemedicine in COVID-19 Response*, *Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response*, and *Guidelines for Workplaces and Establishments Processing Personal Data for COVID-19 Response*. The NPC has likewise issued bulletins on personal data collection in online raffles and games of chance and data privacy best practices in online learning.

Most notably, NPC has recommended the prosecution of the operator of a lending application, which has reportedly been harassing and public-shaming delinquent borrowers, for violating the DPA. It has likewise initiated investigations into the potential data breach of another lending app and a major social media platform.

Singapore

Piyush Gupta, R Saravanan and Wong Zhen
RHTLaw Asia LLP

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

In Singapore, the primary legislation for data protection is the Personal Data Protection Act 2012 (No. 26 of 2012) (the "**PDPA**"). The PDPA provides a general data privacy and protection law that extends to all organizations in the *private* sector. Data management in the *public sector* is governed by the Public Sector (Governance) Act 2018 and the Government Instruction Manual on IT Management.

However, since the intent of this regulatory guide is to assist private entities to explore potential business opportunities in ASEAN, we will focus on the private sector and will only be discussing the provisions under the PDPA hereunder.

The PDPA outlines organizations' obligations in relation to the collection, use, disclosure, access, correction, care, security, retention, and transfer of personal data. It also details Singapore's national Do Not Call ("**DNC**") Registry and organizations' obligations regarding marketing communications to Singapore registered telephone numbers. Subsidiary legislations to the PDPA include regulations relating to, but not limited to, Do Not Call Registry, Enforcement and Notification of Data Breaches. The list of subsidiary legislations can be found at: https://sso.agc.gov.sg/Act/PDPA2012?ViewType=SI.

In addition to the above, there are also other laws and regulations in Singapore that include industry-specific data protection and privacy provisions. Some examples include the Banking Act and the Telecoms Competition Code which is promulgated under the Telecommunications Act. Organizations will have to comply with both the PDPA and the existing sector-specific laws. In the event of any inconsistencies between sector-specific laws and the PDPA, provisions of the sector-specific laws will prevail.

The Monetary Authority of Singapore (MAS) has the power to issue regulations, notices, practice guidelines to the financial sector. The MAS has issued several regulatory instruments that are relevant to data-protection, such as the Technology Risk Management Guidelines, Outsourcing Guidelines and various notices on the theme of Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT). Due to the critical importance of combating money laundering and terrorism financing, the MAS has reminded the financial sector that compliance with the PDPA must not compromise their ability to perform effective customer due diligence. As such, MAS regulations on AML/CFT state that that for the purposes of meeting the AML/CFT requirements, such as in the course of performing customer due diligence, financial institutions may collect, use, and disclose personal data without customer consent, as per existing practice (before the promulgation of the PDPA). This is balanced by customers' rights under the PDPA to access and correct their personal data. Customers will have access to all personal data and the factual identification data that they have provided to the financial institutions.

Singapore

The Personal Data Protection Commission (the "**PDPC**") – The regulatory agency established pursuant to the PDPA – has also established sector-specific advisory guidelines that include, without limitation, the following sectors: education, real estate agencies, and healthcare. These guidelines may be accessed at: https://www.pdpc.gov.sg/Guidelines-and-Consultation?type=sector-specific-advisory-guidelines&keyword=&topic=all&page=1. It may be noted that the guidelines are merely to assist the companies operating in these industries and are non-binding in nature.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

■ Extraterritorial jurisdiction

The broad definition of "organization" under the PDPA applies to organizations collecting, using or disclosing personal data in Singapore, whether or not the organization is physically present in Singapore or is a registered company in Singapore. It therefore means that the PDPA has significant extraterritorial effect.

■ International data transfer

An organization is barred from transmitting personal data of any citizen outside of Singapore unless it complies with the PDPA provisions, which ensure that organizations offer personal data transmitted, a level of security equal to that provided under the PDPA.[1]

An organization may apply to be exempted from any requirement prescribed under the PDPA in relation to transfer of personal data out of Singapore. This exemption may be granted subject to such conditions as the PDPC may specify in writing.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

The PDPC plays the main role in administering and enforcing the PDPA in Singapore. The PDPC has issued several advisory guidelines to provide guidance on the PDPA, although it is to be noted that these advisory guidelines do not have legal force.

The related sectoral regulators implement sector-specific data privacy responsibilities separately. For example, the Monetary Authority of Singapore enforces the Banking Act's banking confidentiality provisions on customers' personal information, and the Info-communications Media Development Authority regulates the confidential treatment of personal information pursuant to the Telecoms Competition Code.

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

It is mandatory for organizations to appoint at least one individual as the DPO to oversee data protection responsibilities and to ensure compliance with the PDPA. The DPO function may be a dedicated responsibility or added to an existing role in the organization. The business contact information of at least one of the DPO must be made available to the public.[2]

The PDPC can take the following enforcement measures against the organization for a failure to appoint a DPO:

(a) Give the organization such instructions as the PDPC deems appropriate in the circumstances to ensure compliance; and/or

(b) Impose a financial penalty of up to SGD1 million (approximately USD760,000) as the PDPC deems appropriate.

[1] Section 26 of the Personal Data Protection Act 2012 (No. 26 of 2012)
[2] Section 11 of the Personal Data Protection Act 2012 (No. 26 of 2012)

Singapore

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

- **Offences and penalties**

  The general penalties stipulated under the PDPA include a fine not exceeding SGD10,000 (approximately USD 7,600) or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding SGD1,000 (approximately USD 760) for every day or part thereof during which the offence continues after conviction.[3]

- **Financial penalties (for contravention of the PDPA not amounting to an offence)**

  If an organization has intentionally or negligently contravened the PDPA provisions, PDPC may impose a financial penalty not exceeding SGD1 million (approximately USD 760,000).[4]

  For any intentional or negligent contravention of the DNC provisions, PDPC may require payment of a financial penalty of up to SGD200,000 (approximately USD 150,000) in the case of an individual and up to SGD1 million (approximately USD 760,000) in any other case.

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

Under the PDPA, a data breach must only be reported if the data breach constitutes a "notifiable breach". A data breach is a notifiable breach if the breach results in, or is likely to result in, significant harm to an affected individual or is of a significant scale. A data breach is deemed to have significant harm to an individual if it relates to any prescribed personal data or classes of personal data and a data breach of significant scale relates to the number of affected individuals affected by the data breach.[5]

If an organization has reason to believe that a data breach has occurred, the organization must assess whether the data breach is a notifiable breach within 30 calendar days. PDPC may take enforcement action against an organization for any unreasonable delay in assessing whether a data breach is a notifiable breach.[6]

If a data breach is determined to be a notifiable breach, the organization must notify the PDPC as soon as is practicable and in any case no later than 3 calendar days after the organization has made the assessment.[7] The notification by the organization to PDPC must be in the form and manner specified on the PDPC's website at www.pdpc.gov.sg / https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, organizations may also contact PDPC at +65 6377 3131 during working hours.

The Personal Data Protection (Notification of Data Breaches) Regulation 2021 sets out the list of information to be included when notifying PDPC of a notifiable data breach.[8] Some key information to include are: how the notifiable data breach occurred, steps taken by the organization after becoming aware of the data breach, the number of individuals affected by the notifiable data breach etcetera.

---

[3] Section 56 of the Personal Data Protection Act 2012 (No. 26 of 2012)
[4] Section 48J of the Personal Data Protection Act 2012 (No. 26 of 2012)
[5] Section 26B of the Personal Data Protection Act 2012 (No. 26 of 2012)
[6] Section 26C of the Personal Data Protection Act 2012 (No. 26 of 2012); Guide on Managing and Notifying Data Breaches under the Personal Data Protection Act
[7] Section 26D of the Personal Data Protection Act 2012 (No. 26 of 2012)
[8] Regulation 5 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021

Singapore

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

A controller / processor of data is also known as a data intermediary in Singapore and there are certain regulatory obligations on a data intermediary. A data intermediary that processes personal data on behalf of another organization pursuant to a contract in writing will be exempt from most of the PDPA obligations except for provisions relating to:

(a) Protection of personal data;

(b) Retention of personal data; and

(c) Notifying the organization of data breaches.

8. Is there a minimum or maximum period for retaining personal data?

Although the PDPA does not set out a specific retention period for personal data, organizations are not allowed to retain personal data in perpetuity. An organization shall not retain personal data as soon as it is reasonable to assume that

(a) The purpose for collection of personal data is no longer being served by retention; and

(b) Retention is no longer necessary for business or legal purposes.[9]

In the financial sector, it is regulatory expectation that personal data is purged from or anonymised in the financial institutions' databases after the minimum retention periods.

9. Are there any exceptions to the local data protection laws?

(a) The following are excluded from the PDPA provisions:

  (i) Any individual acting in a personal or domestic capacity;

  (ii) Any employee acting in the course of his / her employment with an organization; and

  (iii) Any public agency.

(b) The PDPA does not apply to business contact information as well. It is to be noted that the PDPA provisions still apply to the business contact information provided by individuals solely in their personal capacity for personal purposes.

(c) The PDPA does not apply to, or applies to a limited extent to:

  (i) Personal data in a record that has been in existence for at least 100 years and

  (ii) Personal data about a deceased individual who has been dead for more than 10 years.

[9] Section 25 of the Personal Data Protection Act 2012 (No. 26 of 2012)

Singapore

10. What have been the enforcement trends for data protection laws in your jurisdiction?

In general, it appears that aside from issuing advisory notices and directions, PDPC most commonly issues warnings or financial penalties for breaches of the PDPA. Furthermore, organizations that have received warnings or financial penalties from PDPC had mostly breached their protection obligations. This means that these organizations lacked reasonable security measures to protect personal data that is in its possession or under its control.

The most hefty fine imposed till date relates to the notable breach of protection obligation by SingHealth and its IT vendor, Integrated Health Information Systems ("**IHis**") in 2019. PDPC fined both SingHealth and IHis a combined total of SGD1 million (USD 760,000) after PDPC's investigations into the data breach arising from a cyberattack on SingHealth's patient database system. Investigations found that IHis had failed to take adequate security measures to protect the personal data in its possession and this cyberattack was Singapore's most serious breach of public data with the records of 1.5 million patients being leaked.

In the PDPC's Advisory Guidelines to the Enforcement of the Data Protection Provisions (revised 1 February 2021), it was mentioned that disclosure of sensitive personal data (such as medical condition and financial data) in a breach was treated as an aggravating factor and accordingly, a higher penalty was imposed.

PDPC may also accept undertakings from organizations that have potentially contravened the PDPA. This process is intended to allow organizations to implement a plan to rectify the immediate breach and also address any systemic flaws to ensure compliance with the PDPA on a continual basis. Thus far, PDPC has accepted undertakings from some companies including, but not limited to, Grabcar Pte Ltd and HSBC Bank (Singapore) Limited.

South Korea

Timothy Dickens
DR & AJU LLC

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

In South Korea, the Personal Information Protection Act ("**PIPA**") is the overarching personal data law that governs the collection, use, storage and processing of personal information. PIPA is further supplemented by the regulations contained in the Enforcement Decree of PIPA.

There are other sector-specific laws like the Act on the Promotion of Information and Communications Network Utilization and Information Protection Act ("**Network Act**"), Act on the Protection and Use of Location Information, Electronic Financial Services Act etc. There are quite a number of other acts and regulations which contain provisions relating to data protection, which in today's digital world is becoming more prevalent.

In the event of dispute, PIPA would prevail.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

Although PIPA and the Network Act do not specifically address their jurisdictional scope of overseas entities, the Korean regulatory authorities have measures to ensure compliance by overseas entities with these laws.

PIPA covers and regulates international data transfers. PIPA requires personal information controllers to obtain consent for cross-border transfers of personal data to third parties. In instances where the personal information controller is outsourcing personal data to a non-Korean processer, the controller must notify the data subjects of certain information that PIPA prescribes and obtain the data subjects' consent. The controller is also required to enter into an appropriate agreement with the outsourced processor. Furthermore, PIPA applies to all personal information processing entities regardless of where such entities are located, so long as the information collected relates to Korean citizens.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

The Personal Information Protection Commission (the "**PIPC**") enforces PIPA, while the Korea Communications Commission (the "**KCC**") enforces the Network Act.

South Korea

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

The appointment of a Data Protection Officer ("**DPO**") is compulsory in Korea. The penalty for not appointing a DPO would be a fine of up to a maximum of KRW 10 million (approximately USD 9,000).

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

Depending on the breach or non-compliance, the PIPA/Network Act may prescribe corrective orders, administrative fines, penalties as well as criminal sanctions. The sanctions can range in the case of monetary fines anywhere from KRW 10 million (approximately USD 9,000) to KRW 100 million (approximately USD 90,000) while there is also the possibility of criminal sanctions ranging anywhere from two (2) years of imprisonment up to ten (10) years of imprisonment.

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

For data breaches, there is a mandatory duty to report such breach. Both the Network Act and PIPA require a report to be made "immediately" and "without delay". The breaches are to be reported to the PIPC or the Korea Internet and Security Agency (the "**KISA**") via online reporting which in the case of information and communication network infringement incidents is made to https://www.boho.or.kr/consult/hacking.do while personal data breaches are to be reported at https://www.privacy.go.kr/wcp/dcl/spl/splRptInfo.do. The reporting is self-explanatory on the website and very easy to follow.

Network information and communication service providers must report any breach while personal data controllers must report if the data breach involves the personal data of more than 1,000 data subjects.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

PIPA requires personal data controllers to implement detailed technical, managerial, administrative and physical measures such as establishing an internal management plan and safeguards to prevent loss, theft, leaks, destruction of personal information under their control. This includes the following:

(a) Implementing physical safeguards like storage facilities or safety locks for secure data storage;

(b) Installing and upgrading security programs to protect personal data;

(c) Adopting encryption technology and other measures to safely store and transmit personal information;

(d) Establishing and implementing an internal personal information security and management plan; and

(e) Taking measures to prevent forgery or falsification of personal data.

South Korea

8. Is there a minimum or maximum period for retaining personal data?

Although there is no specific period for the retention of personal data under PIPA, this is dependent on the kind of information or data that is stored and varies depending on the applicable act or regulation in certain areas/sectors. The average period for the storage of data is three (3) years but can be up to a period of ten (10) years. For more definitive answers, one would have to look at the kind of data in question and then refer to the applicable act or regulation that will outline the data retention period required.

9. Are there any exceptions to the local data protection laws?

Generally speaking, there are no exceptions to data protection laws in South Korea but Article 18 of PIPA sets out instances where the provisions of consent etc. are not required particularly when it comes to public institutions where data needs to be shared due to:

(a) Necessity of the court to proceed with trial;

(b) Necessity to investigate a crime, indictment and prosecution;

(c) Necessity to enforcement of punishment, probation or custody;

(d) Necessity to provide personal information to a foreign government or international organization to perform a treaty or other international convention; and

(e) Where special provisions of other laws so require.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

From an international perspective, there is coordination and discussions taking place toward enhancing the possibility of receiving a much anticipated adequacy decision from the European Commission which would provide the requisite legal basis for data transfers pursuant to Article 45 of the GDPR. This would also facilitate and accelerate cross-border data transfers and collection of data from EU residents.

Domestically, PIPC announced plans recently to develop an "AI personal information infringement prevention support system" to evaluate whether only a bare minimum of strictly necessary personal information is legitimately being collected under current bills and ordinances.

PIPC announced in early 2021 that it plans to investigate almost 400 infringement cases during the first part of this year. Based on these results, the PIPC plans to issue guidelines for big data service providers and will focus on:

(a) Legality (clearly stating the purpose of the collection and advance consent);

(b) Safety (encryption and de-identification); and

(c) Transparency (relation to scope and duration of the personal data and the AI service).

Taiwan

Eddie Hsiung
Lee and Li

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

Under Taiwan law, the Personal Data Protection Act ("**PDPA**") is the main law governing personal data protection, and the Enforcement Rules of the Personal Data Protection Act ("**Enforcement Rules**") provide further interpretation and implementation of the PDPA. Apart from PDPA-related laws and regulations, there are some other laws and regulations, especially those for specific industry or regulated entities, which also contain personal data-related provisions.

As a principle, in case of any conflict between the PDPA and the personal data-related provisions for specific industry/ regulated entities, the latter (which address the special subject areas) shall prevail because the PDPA is the "general law" for personal data. A ruling issued by Taiwan's Ministry of Justice ("**MOJ**") in 2018 holds the same view.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

Yes, the PDPA has extraterritorial jurisdiction but, according to a ruling issued by the MOJ in 2018, the same is applicable only to collection, processing or use of the personal data of Taiwan individuals by Taiwanese government or Taiwanese non-government entities from outside the territory of Taiwan.

The cross-border transfer of personal data constitutes "international transmission" as defined in the PDPA. According to the PDPA, the competent authority may prohibit a business entity's international transmission of personal data if:

(a) It will prejudice any material national interest;

(b) It is prohibited or restricted under an international treaty or agreement;

(c) The jurisdiction to which the personal data is to be transmitted does not afford sound legal protection of personal data, thereby affecting the rights or interest of the data subjects; or

(d) The purpose of transmitting personal data is to evade restrictions prescribed under the PDPA.

For example, in certain industries such as telecommunications and broadcasting operators, TV channels and cable TV system operators, it is prohibited to transmit customer data to the People's Republic of China.

Taiwan

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

Under Taiwan law, the interpretation authority and enforcement authorities of the PDPA are different.

In January 2019, interpretation authority of the PDPA was changed from the MOJ to the National Development Council (the "**NDC**"), so the NDC is currently the authority in charge of interpreting the PDPA and acts as a coordinator among different government authorities with regard to the interpretation and implementation of personal data protection matters. For example, in response to the implementation of the GDPR, in July 2018, the NDC has already established a Personal Data Protection Office in order to obtain the "adequacy decision" from the EU authority.

The enforcement of the PDPA is carried out by relevant competent government authorities (such as the Financial Supervisory Commission for personal data-related matters of financial institutions). The competent authorities are generally granted the power to enforce certain matters under the PDPA, such as setting out rules with regard to the security maintenance measures of personal data, carrying out audits and inspections, and imposing rectification orders and administrative penalties on the non-government entities under their charge.

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

Although the Enforcement Rules state that a non-government entity shall adopt security and maintenance measures which include allocating management personnel and reasonable resources, the PDPA does not require a non-government entity to appoint a DPO. The appointment of a DPO is therefore optional.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

A non-government entity's non-compliance with the PDPA may result in, for example, the following:

(a) Civil liability
Any non-government entity should be liable for damages caused to a data subject arising out of unlawful collection, processing or use of personal data.

(b) Administrative liability
Any violation of the PDPA may result in administrative liability. For example, failure to obtain necessary consent from the data subject before collecting, processing or using his/her personal data as required by the PDPA by a non-government entity may be subject to an administrative fine between NTD50,000 (approximately USD 1,800) and NTD500,000 (approximately USD 18,000).

(c) Criminal liability
An individual (i.e., natural person) would be subject to imprisonment for no more than five (5) years and/or a criminal fine no more than NTD1 million (approximately USD 36,000) in case of a violation of certain provisions under the PDPA (such as failure to obtain necessary consent from the data subject before collecting, processing or using his/her personal data as required by the PDPA) with the intention of obtaining unlawful profit or impairing the interests of others.

Taiwan

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

The PDPA does not require the reporting of data breaches to relevant data protection authorities. However, there may be such mandatory requirement for data breaches to be reported to the relevant supervisory authority under the laws and regulations for specific industry sectors or regulated entities. For example, the Financial Supervisory Commission (the "**FSC**"), the competent authority in charge of the financial services industry, requires in its "Regulations Governing Maintenance of Personal Information Files by the Non-government Institutions as Designated by the Financial Supervisory Commission" that financial institutions under the FSC's supervision shall report the occurrence of any material data incident to the FSC. The process or form that needs to be completed when submitting a report shall depend on the relevant rules applicable to the specific industry sectors or regulated entities, but as a general principle and in practice, the report shall be in a written form.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

Please see below certain continuing / ongoing regulatory obligations under the PDPA:

(a) Security measures

The PDPA requires non-government entities to adopt appropriate security measures to protect personal data from being stolen, altered, damaged, destroyed, lost or disclosed. The Enforcement Rules provide that such measures shall be proportionate to the intended purposes of personal data protection, and may include items such as:

(i) Allocation of management personnel and reasonable resources;

(ii) Mechanism of risk assessment and management of personal data;

(iii) Establishing a mechanism of preventing, giving notice of, and responding to a data breach;

(iv) Establishing an internal control procedure for the collection, processing, and use of personal data, etc.

(b) Report to data subjects in case of data incidents

If any personal data is stolen, disclosed, altered, or otherwise infringed upon due to non-compliance with the PDPA by a non-government entity, the non-government entity must notify the data subject of the incident and the remedies that the non-government entity has adopted as soon as the non-government entity has carried out an investigation of the incident.

(c) Supervision of party commissioned to collect, processing or use of personal data

A controller, when commissioning another to collect, process or use personal data, such controller shall properly supervise the commissioned party.

Taiwan

8. Is there a minimum or maximum period for retaining personal data?

The PDPA does not expressly provide for a minimum or maximum period for retaining personal data. However, pursuant to the PDPA, a non-government entity shall, voluntarily or upon the request of the data subject, delete or stop collecting, processing or using personal data when the purpose(s) for which the personal data were collected cease(s) to exist or when the retention period (the information that the data subject should be informed of when his/her personal is being collected) expires, subject to some exemptions specified in the PDPA.

9. Are there any exceptions to the local data protection laws?

While the PDPA should apply to any collection, processing and use of personal data (as defined under the PDPA), Article 51 of the PDPA expressly provides that the PDPA shall not apply in the following two circumstances:

(a) The collection, processing or use of personal data by natural persons for the purpose of purely personal or family activities; or

(b) Audio-visual data collected, processed, or used in public places or public activities and not connected to other personal data.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

Although the PDPA applies to all business activities (where any personal data is involved), our observation is that more enforcement cases are related to specific industry sections that are more regulated, such as financial services. For financial industry, personal data protection has become an area that the FSC, Taiwan's financial regulator, would focus when the FSC is conducting financial examination on the financial institutions. According to the official website of the FSC's Financial Examination Bureau, the recent main defects of financial institutions with respect to personal data protection include, for example, failure to adopt appropriate operational and control procedure for providing customer's personal data to a third party, failure to adopt sufficient security maintenance measures for protecting customers' data such as giving personnel (who does not have a need) access to a bank's core system, which keeps a large amount of personal data. There have been cases of disciplinary actions (e.g., administrative fines) against financial institutions due to their defects with respect to personal data protection.

Thailand

Picharn Sukparangsee
Bangkok Global Law

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

Personal Data Protection Act, B.E. 2562 (A.D. 2019) or the PDPA will come into full effect on 1 June 2022. The PDPA is implemented to provide standards to directly protect personal data from unauthorised or unlawful collection, use, or disclosure and processing of any data from the data subject.

Computer Crime Act B.E. 2560 (2017), provides for penalties on computer crimes. With the use of proxy servers and other easily obtainable tools, hackers and cyber offenders are difficult to investigate with everyday technological solutions. As a result, Computer Crime Act has been enacted to prevent and suppress criminal offences involving computer / cyber crimes, including loss of data.

In the event of a breach of personal data protection, provisions of the PDPA are applicable.

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

The Thai PDPA does not have extraterritorial jurisdiction.

Pursuant to Section 5 of the PDPA, in case there are connecting factors or links, the scope of enforcement of the PDPA is extended to any data controller and any data processor who is outside of Thailand, but the data subject is in Thailand and each of the data controller and the data processor engages in any of the following activities:

(a) Offering of goods or services to the data subject who is in Thailand, irrespective of whether the payment is made by the data subject; and/or

(b) Monitoring of the data subject's act, where the act takes place in the Thailand.

According to Section 28 of the PDPA regarding international data transfer, the personal data of the data subject may be transferred to a foreign country when the destination country or international organization has adequate data protection standard.

The power to determine whether or not the destination country or international organisation has the adequacy of personal data protection is vested to the Personal Data Protection Commission (the "**Commission**").

It should be noted that the transfer of personal data may not be subjected to Section 28 if such transfer falls into these following exemptions:

(a) It is necessary for compliance with laws;

(b) Where the consent of the data subject has been obtained, provided that the data subject has been informed of the inadequate personal data protection standards of the destination country or international organization;

(c) It is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

(d) It is for compliance with a contract between the Data Controller, and other Persons or juristic persons for the interests of the data subject;

(e) It is to prevent or suppress a danger to the life, body, or health of the data subject or other persons, when the data subject is incapable of giving the consent at such time; or

(f) It is necessary for carrying out the activities in relation to substantial public interest.

However, it should be noted that Section 29 of the PDPA also allows international transfers of personal data where the personal data is transferred between the data controller and the data processor which are an affiliated company or are in the same group of companies and such group of companies has policy to protect personal data during transfer as approved by the Commission.

In case the policy of protection of personal data has been approved by the Commission, or in case the international transfer meets any of the aforementioned (1)-(6) exemptions, the data controller and the data processor may transfer personal data to a third country only under appropriate measures, as well as efficient legal remedial measures in accordance with guideline as announced by the Commission.

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

The Minister of Digital Economy and Society (the "**MDES**") is in charge of the PDPA, and has the power to appoint competent officials to perform acts under the PDPA.

The PDPA establishes the Commission to enforce the PDPA. Also, the PDPA empowers the Commission to appoint committees or sub-committees for considering or performing any act as prescribed by the Commission.

According to Section 16 of the PDPA, the Commission is mainly responsible to issue specific regulations under the PDPA, determine measures or guidelines of the operation of personal data, render official interpretation and announce orders in connection with the PDPA.

Thailand

4. Is the appointment of a Data Protection Officer ("DPO") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

Pursuant to Section 41 of the PDPA, the Data Protection Officer or the DPO shall be provided in the following circumstances:

(a) The data controller or the data processor is a public authority as prescribed and announced by the Commission;

(b) The activities of the data controller and the data processor in the collection, use or disclosure of the personal data require monitoring of the personal data or the system by the reason of having a large number of personal data as prescribed by the Commission; or

(c) The core activity of the data controller or the data processor is to collect, use, or disclose sensitive personal data as specified in Section 26 of the PDPA.

The sensitive data under Section 26 of the PDPA includes racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, 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.

It should be noted that if the data controller and the data processor are in the same affiliated companies, the DPO may be jointly provided.

The failure of designation of the DPO may lead the data controller and the data processor to administrative fine of not exceeding THB 1 million (approximately US 32,000) each in accordance with Section 82 of the PDPA.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

Any non-compliance or violation of the PDPA may lead to criminal liability and administrative liability.

(a) Civil liability
Imprisonment of up to one (1) year and fines of up to THB 5 million (approximately USD 160,000) or both. The key performances which may lead the data controller and the data processor to the criminal penalty are as follows:

(i) A data controller who uses or discloses personal data or sends sensitive personal data outside of Thailand in violation of the law in a manner that is likely to cause other person to suffer any damage, impair his or her reputation, or expose such other person to be scorned, hated, or humiliated, or to illegally acquire benefits; and

(ii) Any person who acquires knowledge of personal data due to the duties under the PDPA and disclose it to another person.

(b) Administrative liability
The amount of fine is dependent on the severity of the violation. The maximum administrative fine imposed by the authority for the violation of the PDPA can be up to THB 5,000,000 (approximately USD 160,000).

Thailand

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

According to Section 37 (4), the PDPA stipulates that the data controller shall notify to the Office of the Personal Data Protection Commission (the "**Office**") any personal data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such personal data breach is unlikely to result in a risk to the rights and freedoms of the persons. However, in case the breach is likely to cause a risk to the rights and freedoms of the data subject, the data controller is obliged to notify without delay the data subject as well.

In case the personal data breach occurs when the personal data is being processed by the data processor, Section 40 (2) requires the data processor to notify the data controller of the personal data breach that occurred. In this regard, the data processor is responsible to provide appropriate security measures for preventing unauthorized or unlawful loss, access to, use, alteration, correction or disclosure, of the personal data.

It should be noted that the PDPA allows the data subject to file with the Office a complaint against the data controller or the data processor in case his/her data has been misused.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

The PDPA specifies the duties and responsibilities for the data controller and the data processor to oblige as set forth below.

- **Personal Data Controller**

  As to Section 37 of the PDPA, the data controller shall comply with the following duties:

  (a) Providing appropriate security measures for preventing unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of the personal data. The measures must be reviewed in accordance with the change of the technology;

  (b) Taking action to prevent the person receiving the personal data from unlawfully using or disclosing the personal data once the personal data is provided to such person, apart from the data controller and the data processor;

  (c) Putting in place the examination system for erasure or destruction of the personal data when the personal data retention period ends or when the personal data is irrelevant or unnecessary including upon the request to delete the personal data from the data subject;

  (d) Notifying the Office of any personal data breach without delay and, where feasible, within 72 hours after having become aware of it; and

  (e) Appointing a representative of the data controller in writing who must be in Thailand to be authroised to act on behalf of the data controller in case the data controller is outside of Thailand. Such representative of the data controller shall be designated without any limitation of liability with respect to the collection, use or disclosure of the personal data according to the purposes of the data controller.

- **Personal Data Processor**

  As to Section 40 of the PDPA, the data processor shall comply with the following duties:

  (a) Carrying out the activities related to the collection, use, or disclosure of the personal data under instruction of the data controller;

  (b) Providing appropriate security measures to prevent unauthorized or unlawful loss, access to, use, alteration, correction or disclosure of the personal data; and

  (c) Preparing and maintaining records of personal data processing activities in accordance with the rules and procedures as set forth by the Commission.

8. Is there a minimum or maximum period for retaining personal data?

The PDPA is silent on a specific retention period for the personal data. However, pursuant to Section 23(3) of the PDPA, the data controller is required to notify data subject prior to or at the time of the personal data collected about the period for which the personal data will be retained. In case it is not possible to specify the retention period, the expected data retention period according to the data retention standard shall be specified. In addition, the data controller shall also put in place the examination system for erasure or destruction of the personal data when the retention period ends, or when the personal data is irrelevant or beyond the purpose necessary for which it has been collected.

Furthermore, the data subject may exercise his/her right under Section 33 of the PDPA to request the data controller to erase or destroy or anonymise his/her personal data.

Therefore, even the PDPA does not specify the period for retention of the personal data, however, according to the aforementioned explanation, the data controller shall no longer have right to retain the personal data when the retention period expires, or the personal data is no longer necessary in relation to the purposes for which such personal data was collected, or the personal data is requested by the data subject to be erased, destroyed or anonymised.

9. Are there any exceptions to the local data protection laws?

Section 4 of the PDPA stipulates the PDPA shall not apply to:

(a) Collection, use or disclosure of the personal data for personal benefit or household activity of a person only;

(b) Operations of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity;

(c) The uses or disclosure of the personal data that is collected only for the activities of mass media, fine arts, or literature, which are only in accordance with professional ethics or for public interest;

(d) The House of Representatives, the Senate, and the Parliament, including the committee appointed by the House of Representatives, the Senate, or the Parliament, which collect, use or disclose the personal data in their consideration under the duties and power of the House of Representatives, the Senate, the Parliament or their committee, as the case may be;

(e) Trial and adjudication of courts and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure; and

(f) Operation of data undertaken by a credit bureau company and its members, according to the law governing the operations of a credit bureau business.

It should be noted that the Royal Decree may be promulgated in the future if there are any other exemption to any other business or entities engaging in a similar manner to the exceptions as specified above.

The businesses that are exempted under the PDPA or the Royal Decree is still required put in place a security protection of the personal data in accordance with the standards.

10. What have been the enforcement trends for data protection laws in your jurisdiction?

Currently, there are many regulations, rules and guidelines under the PDPA awaiting to be issued. However, the Government of Thailand expects all business entities to start taking action for compliance with provisions of the PDPA such as classifying all information, creating the platform to keep and organize the personal data including arranging and maintaining security for protection of the personal data.

Business entities including organizations dealing with personal data of their clients or customers are alerted with concerns about the PDPA as the grace period will end on 31st May 2021. Although the MDES is trying to accelerate issuance of subordinate rules and regulations under the provisions of the PDPA, small and medium-sized businesses, or SMEs are not quite ready as they should be as it requires a lot of investment in both personnel and technology. Moreover, this same facet of the Thai economy has been suffering from the effects of COVID-19. Despite the government recognizing the urgency of PDPA, the actual application and enforcement of it may be slower than initially anticipated.

Vietnam

Benjamin Yap and Mai Thi Ngoc Anh
RHTLaw Vietnam

1. Is there a specific data protection law in your jurisdiction? If so, are there any other laws which also contain provisions relating to protecting data (e.g. telecom laws etc)? If so, in the event of a dispute, which law would prevail?

There is no specific data protection law in Vietnam. Data is generally protected on a piecemeal basis under the following laws:

(a) Civil Code No. 91/2015/QH13 dated 24 November 2015 ("**Civil Code**");

(b) Law on Cyber Information Security No. 86/2015/QH13 dated 19 November 2015 ("**Law on Cyber Information Security**");

(c) Law on Information Technology No. 67/2006/QH11 dated 29 June 2006 ("**Law on Information Technology**");

(d) Law on Cybersecurity No. 24/2018/QH14 dated 12 June 2018 ("**Law on Cybersecurity**");

(e) Law on Protection of Consumer Rights No. 59/2010/QH12 dated 17 November 2010 as amended in 2017 ("**Law on Protection of Consumer Rights**");

(f) Law on Telecommunication No. 41/2009/QH12 dated 23 November 2009 ("**Law on Telecommunication**");

(g) Law on Electronic Transactions No. 51/2005/QH11 dated 9 December 2005 ("**Law on Electronic Transactions**");

(h) Law on Post No. 49/2010/QH12 dated 17 June 2010 ("**Law on Post**");

(i) Law on Publication No. 19/2012/QH13 dated 20 November 2012, as amended in 2018 ("**Law on Publication**");

(j) Law on Press No. 103/2016/QH13 dated 05 April 2016, as amended in 2018 ("**Law on Press**").

There is no conflict since there is no specific data protection law. Generally therefore:

(a) A later law repeals an earlier law[10];

(b) Special law repeals general law[11].

[10] *Article 156.3 of the Law on Promulgation of Legislative Documents No. 80/2015/QH13 dated 22 June 2015*
[11] *Article 4 of the 2015 Civil Code*

Vietnam

2. Does the data protection law in your country have extraterritorial jurisdiction? Does it also cover international data transfer?

Yes. The Vietnamese laws cover extraterritorial jurisdiction[12]. Data protection provisions highlighted above apply also to foreign individuals / entities. The current Vietnamese data protection laws are silent on international data transfer. However, currently, the government is drafting a decree on personal data protection ("**Draft Decree**") which includes the provision on international data transfer. It is expected that such Draft Decree shall be issued and take effect by the end of this year[13].

3. Which authority(ies) is/are responsible for enforcing data protection laws in your jurisdiction?

Under the Vietnamese laws, the following authorities are responsible for enforcing data protection laws:

(a) Ministry of Public Security;[14]

(b) Ministry of National Defense;[15]

(c) Ministry of Information and Communications;[16] and

(d) Ministry of Industrial and Trade[17].

4. Is the appointment of a Data Protection Officer ("**DPO**") compulsory or optional? If the appointment of a DPO is compulsory, what are the penalties for failing to appoint a DPO?

There is currently no provision for the appointment of a DPO.

5. What are the penalties for non-compliance with the data protection laws in your jurisdiction?

Non-compliance with the Vietnamese data protection laws may attract: (a) administrative penalties which may range from VND 30,000,000 (approximately USD 1,300) to VND 70,000,000 (approximately USD 3,000) or (b) criminal penalties which may include an imprisonment sentence ranging from six (6) months to seven (7) years; or (c) a prohibition from holding certain positions or doing certain jobs from one (1) to (5) years; or a fine which may range from VND 50,000,000 (approximately USD 2.250) to VND 1,000,000,000 (approximately USD 45,000), or a sentence of non-custodial reform of up to three (3) years.

---

[12] *Article 663.2 of the Civil Code; Article 2 of 2006 Law on Information Technology, Article 2 of 2015 Law on Cyber information Security; Article 26.3 of the Law on Cybersecurity*
[13] *http://news.chinhphu.vn/Home/Personal-data-protection-to-be-decreed/202010/41695.vgp*
[14] *Article 36 of the 2018 Law on Cybersecurity*
[15] *Article 37 of the 2018 Law on Cybersecurity*
[16] *Article 38 of the 2018 Law on Cybersecurity, Article 6.2 of the Law on Publication, Article 47.2 of the Law on Post, Article 8.2 of the Law on Electronic Transactions; Article 7.1 of the Law on Press, Article 9.2 of the Law on Telecommunication, Article 7.2 of the Law on Information Technology*
[17] *Article 47.2 of the Law on Protection of Consumer Rights*

Vietnam

6. Is there a mandatory requirement for data breaches to be reported to any authority? If so, when does the obligation arise? What information should be provided when notifying the authority(ies)? Is there a standard process or form that needs to be completed when submitting such notification?

The current Vietnamese laws are silent on this issue. However, as mentioned in the response to Question 2 above, Draft Decree requires the relevant individual / entity to notify the Committee for protection of personal data regarding any violations relating to personal data protection.[18] However, the Draft Decree still does not have any provision regarding the time when the notification obligation arises or what information should be provided when notifying the authority or a standard process or form that needs to be completed when submitting such notification.

7. Are there any continuing / ongoing regulatory obligations by controllers / processors of data under the data protection laws in your jurisdiction?

Under the Vietnamese laws, generally, organizations and individuals that process personal information must comply with the following provisions[19]:

(a) Collect personal information only after obtaining the consent of its owners regarding the scope and purpose of collection and use of such information;

(b) Use the collected personal information for purposes other than the initial one only after obtaining the consent of its owners; and

(c) Refrain from providing, sharing or spreading to a third-party personal information they have collected, accessed or controlled, unless they obtain the consent of the owners of such personal information or at the request of competent state agencies.

8. Is there a minimum or maximum period for retaining personal data?

The Vietnamese laws do have a provision regarding "the retention of personal data"[20]. However, there is no provision clarifying the specific period for which the personal data can be retained.

9. Are there any exceptions to the local data protection laws?

Yes. According to Article 26.3 of the Law on Cybersecurity, the following entities carrying out activities of collecting, exploiting, analyzing and processing data being personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a specified period to be stipulated by the Government:

(a) Domestic and foreign service providers on telecom networks and on the Internet; and

(b) Cyberspace service providers and other value-added cyberspace service providers in Vietnam.

Such foreign enterprises must have branches or representative offices in Vietnam.

---

[18] *Article 28.3 of the Draft Decree*
[19] *Article 6.4 of the Law on Telecommunications; Article 17 of the Law on Cyber information Security*
[20] *Article 18.3 of the Law on Cyber Information Security*

Vietnam

10. What have been the enforcement trends for data protection laws in your jurisdiction?

There seems to be increased activity in data protection in Vietnam though enforcement of data protection laws have yet to be a priority. It is hoped that with the passing of the Draft Decree, this will change.

On 9 February 2021, the Ministry of Public Security released the second version of the Draft Decree on personal data protection to collect public opinions. The Draft Decree sets out rules regulating specific rights of data subjects, cross-border transfer of data, and processing of sensitive personal data. Non-compliance penalties include temporary suspension of operation, and/or revocation of permission for cross-border data transfer in addition to monetary fines.

Authors

Vannak Houn
Managing Partner
vannak.houn@rhtlawcambodia.com
Cambodia

Liow Yee Kai
Of Counsel
yeekai.liow@rhtlawasia.com
Cambodia

Henry Huang
Managing Partner
huangningning@grandall.com.cn
China

Nicole Jiang
Lawyer
jiangyuanxiu@grandall.com.cn
China

Anant Merathia
Managing Partner
anant@merathiacorp.com
India

Poornima Devi
Associate
poornimadevi@merathiacorp.com
India

Genio Atyanto
Partner
atyanto@nacounsels.com
Indonesia

Mohanthas Narayanasamy
Partner
mohansamy@pcalaw.com.my
Malaysia

Franchette M. Acosta
Senior Partner
fm.acosta@thefirmva.com
Philippines

Imperial, Paul Rodulfo B.
Partner
pb.imperial@thefirmva.com
Philippines

Piyush Gupta
Partner (Foreign Lawyer)
piyush.gupta@rhtlawasia.com
Singapore

R Saravanan
Associate
saravanan.r@rhtlawasia.com
Singapore

Wong Zhen
Practice Trainee
zhen.wong@rhtlawasia.com
Singapore

Timothy Dickens
Senior Foreign Attorney
tjldickens@draju.com
South Korea

Eddie Hsiung
Associate Partner
eddiehsiung@leeandli.com
Taiwan

Picharn Sukparangsee
Managing Partner
picharn@bgloballaw.com
Thailand

Benjamin Yap
Senior Partner
benjamin.yap@rhtlaw.com.vn
Vietnam

Mai Thi Ngoc Anh
Partner
anh.mai@rhtlaw.com.vn
Vietnam