Protection and Cross-border Transfer of Personal Information in the Asia Pacific - 2018

This handbook provides guidance for the protection and cross-border transfer of personal information in the Asia Pacific region and has been prepared by Multilaw lawyers with expertise in data protection practice in the region.

Due to the importance of personal information both for businesses and individual rights thereunder, Asia Pacific countries implemented laws and regulations for the protection of personal information and restriction on its transfer to third countries, similar to the GDPR.

This guidance is useful especially for business entities that process personal information in Asia Pacific countries or transfer it from or to Asia Pacific countries.

Answers to the following questions are provided by Multilaw member firms in Australia, China, Hong Kong, Indonesia, Japan, Malaysia, New Zealand, Pakistan, Philippines, Singapore, South Korea, Sri Lanka, Taiwan, Thailand and Vietnam.

Due to the rapidly changing laws and regulations for protection of personal information, each law firm author should be contacted for updates.

Please note that information provided is intended to provide general information on the protection of personal information as of **end of February 2018**. It is not, and does not constitute, specific legal advice.

Editor: Hiroyasu Kageshima – Partner, Ushijima & Partners, Japan
hiroyasu.kageshima@ushijima-law.gr.jp

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Q4 Consent for Acquisition or Usage

(1) Is consent from the data subject required to acquire P.I.?
(2) Is consent from the data subject required to use P.I.?

Q5 Consent for Provision

Is consent from the data subject required to provide P.I. to a third party?

Q6 Exceptions for Consent

What are the major exceptions to Q4 and Q5 above?

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

Q11 Security Control

What are the major rules for security control of P.I.?

The general view of legal restrictions under current legal rules in each country /region is as outlined in the following table.

	Specific Law	Sensitive Information	Consent for Acquisition, Usage	Consent for Provision	Information to be Provided	Transfer to Third Countries	Data Localization	Security Control
Australia	✓	✓	✓	✓	✓			✓
China	✓	✓	✓	✓	✓	✓	✓	✓
Hong Kong	✓	✓	✓	✓	✓	✓		✓
Indonesia			✓	✓	✓			✓
Japan	✓	✓		✓	✓	✓		✓
Malaysia	✓	✓	✓	✓	✓	✓		✓
New Zealand	✓		✓	✓	✓	✓		✓
Pakistan								
Philippines	✓	✓	✓	✓	✓			✓
Singapore	✓		✓	✓	✓	✓		✓
South Korea	✓	✓	✓	✓	✓	✓		✓
Sri Lanka								
Taiwan	✓	✓	✓	✓	✓	✓		✓
Thailand								
Vietnam			✓	✓	✓	✓		✓

Australia

Macpherson Kelley Lawyers

Address: 40-42 Scott Street, Dandenong, Victoria, 3175
Level 22, 114 William Street, Melbourne, Victoria, 3000
Paul Kirton - Legal Practice Principal
Phone: +61 (3) 9794 2621
Mobile: +61 0419 754 877
Email: paul.kirton@mk.com.au
Kelly Dickson - Principal Lawyer
Phone: +61 (3) 9794 2541
Mobile: +61 0419 754 860
Email: kelly.dickson@mk.com.au

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) There is no express right in the Australian Constitution for privacy or data protection. Instead, regulation of privacy and data protection rights is contained in a range of different federal and state based laws.

The primary federal legislation in Australia is the Privacy Act 1988 (Cth) (Privacy Act), which regulates "personal information" held about individuals. It includes thirteen Australian Privacy Principles (APPs) which set out the standards, rights and obligations for the use, disclosure, handling, storing, destruction, access and correction of personal information. The Privacy Act covers both the public and private sectors. The Privacy Act also regulates credit reporting.

Each Australian State/Territory also has its own privacy legislation dealing with the public sector:

* Information Privacy Act 2014 (Australian Capital Territory)
* Information Act (Northern Territory)
* Privacy and Personal Information Protection Act 1988 (New South Wales)
* Privacy and Data Protection Act 2014 (Victoria)
* Personal Information and Protection Act 2004 (Tasmania)
* Information Privacy Act 2009 (Queensland).

Western Australia and South Australia do not currently have a specific legislative privacy regime (although South Australia has an administrative instruction requiring compliance with a set of Information Privacy Principles, and Western Australia has some privacy principles covered in the Freedom of Information Act 1992 (Western Australia)).

There is also specific legislation dealing with "health information" in each State and Territory.

(2) The federal Privacy Act commenced in 1988, and has been amended at various times, most notably being:

* 2000 (extending the application of the privacy regime from the public sector to also include many enterprises in the private sector);
* 2010 (amending and enhancing the privacy regime);
* 2018 (implementing a mandatory data breach notification regime).

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Under the federal Privacy Act, "personal information" is broadly defined as "information or an opinion about an identified individual, or about an individual who is reasonably identifiable:

* whether the information or opinion is true or not; and
* whether the information or opinion is recorded in a material form or not."

The definition of "personal information" also includes specific sub-sets of information (e.g. "sensitive information" and "health information" - see further our answer to question 3 below).

In the consumer credit space, there are also particular definitions relating to "credit information" and "credit eligibility information", etc.

The definition of "personal information" is broad enough to include personal information held about individuals in a business capacity (e.g. the name, phone number and email address of a business supplier). The key is simply whether the information can identify an individual, either on its own, or when collated with other facts.

The federal Privacy Act does not apply to personal information held in employee records, where:

* the employee record is held only by the employing entity; and
* the use of the personal information is directly related to a current or former employment

relationship.

The privacy legislation in each State and Territory also has separate (and sometimes differently-worded) definitions for "personal information".

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Under the federal Privacy Act, "sensitive information" is defined as "information or an opinion about an individual's racial or ethnic origin, political opinions, political association membership, religious beliefs or affiliations, philosophical beliefs, professional or trade association membership, trade union membership, sexual orientation or practices or criminal record, health information and genetic information".

"Health information" is defined as:

* information or an opinion about the health or a disability (at any time) of an individual; or an individual's expressed wishes about the future provision of health services to him or her, or health services provided or to be provided to an individual, that is also personal information; or
* other personal information collected to provide, or in providing, a health service; or
* other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
* genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

The privacy legislation in each State and Territory also has separate (and sometimes differently-worded) definitions for "sensitive information" and "health information".

Q4 Consent for Acquisition or Usage

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) Sometimes consent is required, sometimes not.

Depending on whether the collecting entity is a government agency or a private sector organisation, personal information must only be collected if it is reasonably necessary for (and

sometimes directly related to) the entity's functions or activities.

An entity must only collect sensitive information if:

* the individual consents, AND it is reasonably necessary for (or directly related to) the entity's functions or activities; OR
* a permitted collection situation exists (see further our answer to question 5 below).

(2) Sometimes consent is required, sometimes not.

If an entity holds personal information about an individual that was collected for a particular (primary) purpose, then the entity must not use that information for another (secondary purpose) unless:

* the individual has consented; OR
* a permitted usage situation exists (see further our answer to question 5 below).

Q5 Consent for Provision

Is consent from the data subject required to provide P.I. to a third party?

Not specifically. However, at or around the time of collection of the data, an entity is broadly required to notify individuals of certain matters, specifically including the detail of any third parties to whom the entity usually discloses personal information of the kind collected.

Consent would be required if the contemplated disclosure is not for a primary purpose and does not fall within the permitted exceptions.

Q6 Exceptions for Consent

What are the major exceptions to Q4 and Q5 above?

Personal information, sensitive information and health information can variously be collected, used and disclosed in "permitted" situations. These typically include:

* as required or authorized by law or Court order;
* as required for Government enforcement-related activities;
* as required to investigate and resolve reasonable suspicions of unlawful activity;
* for the purposes of establishing and defending valid legal and equitable claims; and
* where there is a reasonable belief that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health

or safety.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

At or before the time of collection of personal information, or if that is not practicable then as soon as practicable thereafter, an entity must take such steps as are reasonable in the circumstances to notify the individual of certain matters. These are:

* the identity and contact details of the entity;
* if the entity has collected the personal information from a third party - the fact that the entity has so collected the information and the circumstances of the collection;
* if the collection of the information is required or authorized by law or Court order – the fact that the collection is so required (including details);
* "why" the entity collects the information;
* the main consequences for the individual if some or all of the information is not collected;
* "who" the entity typically discloses such personal information to;
* detail about "how" an individual can access the information held about them;
* detail about "how" an individual can seek the correction of the information held about them;
* detail about "how" an individual can complain about an actual or suspected breach of their privacy; and
* whether the entity is likely to disclose the information to overseas recipients (including a list of the likely countries of disclosure).

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

No. However, before an entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas entity will not breach the 13 APPs. A breach by the overseas entity will typically be treated as a breach by the local (disclosing) entity and liability will flow to the local (disclosing) entity.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

The local (disclosing) entity's obligation to take reasonable steps as set out in question 7 above

does not apply if:

* the entity reasonably believes that the overseas recipient is subject to a binding privacy regime that is at least substantially similar to the protections afforded to the individual under the Australian regime AND the individual can take local enforcement action for protection in the foreign country; OR
* the entity expressly obtains informed consent from the individual, including an express acknowledgement from the individual that it understands that, by providing consent, the entity's local liability will be extinguished; OR
* the overseas disclosure is required or authorized by law; OR
* a permitted disclosure situation exists; or
* (for governmental agencies) the disclosure is required by international treaty or for enforcement-related activity.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

No. Although there are obligations on an entity that holds personal information to allow access and correction of that information in certain circumstances, and to take reasonable steps to protect and keep the information current, accurate and secure.

Q11 Security Control

What are the major rules for security control of P.I.

Australian entities subject to the federal Privacy Act must:

* implement practices, procedures and systems that will ensure compliance with the Privacy laws;
* train staff;
* have and maintain a Privacy Policy (containing mandated content);
* notify individuals about the collection of their personal information (see our answer to question 6 above);
* take reasonable steps to ensure that the personal information held, used and disclosed is accurate, up to date and complete;
* take reasonable steps to protect the information from misuse, interference and loss;
* take reasonable steps to protect the information from unauthorized access, modification or disclosure;
* take reasonable steps to destroy or de-identify information when it is no longer needed;

* comply with processes for allowing access to, and correction of, personal information; and
* (as of 22 February 2018) report "eligible data breaches" to the Australian Privacy Commissioner and affected individuals.

"Reasonable steps" in relation to security include consideration of:

* physical data security measures;
* electronic data security measures (eg. computer and network security);
* communications security protocols;
* personnel security;
* contractual obligations imposed on, and due diligence of, contractors and third parties;
* destruction protocols; and
* critical incident response plans.

In determining the “reasonableness” of an entity's Privacy compliance measures, a range of factors can be considered. However, an entity is not excused from taking certain actions by reason only that it would be inconvenient, time-consuming, difficult or impose some cost to do so. Whether these factors make it “unreasonable” to take a particular step will depend on whether the burden is excessive in all the circumstances, considering the size of the business, the type of information held, and the likely risks to individuals etc.

China

JunHe LLP

Marissa Dong: Dongx@junhe.com
Guo Jinghe: Guojh@junhe.com

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. "Cyber Security Law of the People's Republic of China" (CSL) is the law.
(2) Enforced in 1 June 2017.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Personal information shall refer to various types of information that can be used separately or in combination with other information to identify a natural person, including but not limited to the name, date of birth, identity certificate number, personal biological identification information, address, telephone numbers, etc. of the natural person.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

The CSL or other laws and regulations do not define the category of sensitive P.I., yet according to *Information security technology-Personal information security specification* (**P.I. Specification**), a recommendable national standard enforced on 1 May 2018 provides that personal sensitive information shall refer to personal information the leakage, disclosure, or abuse of which could easily endanger personal and property safety, and easily lead to the harm of one's personal reputation and mental & physical health, or lead to discriminatory treatment. Generally, the personal information of children under 14 years of age and the private information of natural persons shall fall under Personal Sensitive Information, and the sensitive information is divided into categories of 'Personal property information', 'Pathological and health information', 'Personal biometric information', 'Personal identity information', 'Network identity information' and 'Other information'.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) Yes.

(2) Yes.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

Yes.

Q6 **Exceptions for Consent**

What are the major exceptions to Q4 and Q5 above?

The PRC laws and regulations do not specifically provide for exceptions to 4 and 5 above. Under the P.I. Specification, there is no need to obtain a consent from personal information subject in the following circumstances, yet whether they will be accepted by regulators in practice may be decided on a case by case basis:

(i) Personal information is related directly to national security or national defense.

(ii) Personal information is related directly to public security, public health or critical public interests.

(iii) Personal information is related directly to the investigation, prosecution, trial and ruling execution of criminals.

(iv) There is a need to protect critical legal interests such as human life or fortune, and it is difficult to obtain consent of the personal information subject.

(v) Personal information is disclosed by the personal information subject voluntarily.

(vi) Personal information is collected through legally public disclosed information channels, such as news report, disclosed government information.

(vii) Personal information is necessary to collect because the personal information subject ask for signing and performance contract.

(viii) Personal information is necessary to maintain the operation security and stability of the product or service provided to personal information subject, such as the fault discovery and management of the product or service.

(ix) The personal information controller is a news report work unit, and the personal

information is necessary for news report.

(x) The personal information controller is an academic research organization, and the personal information is necessary for statistics or academic research, and when publicly providing the results of the research, the information contained in the results shall be de-identificated.

(xi) Other situations formulated in laws and regulations.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

The CSL generally requires that the purposes, methods and scope of the information collection and use shall be clearly indicated, yet the specific requirement is not provided.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

According to the CSL and its ancillary rules, requirements on data localization and security assessment for data exports mainly apply to two types of entities, i.e. the critical information infrastructure operator and the network operators.

Also, according to the CSL, personal information and important business data collected and generated in the operation of critical information infrastructures operators within the territory of the People's Republic of China shall be stored within the territory. Where it is necessary to provide such information and data abroad due to business needs, security assessment shall be carried out according to the measures formulated by the national Internet information department in conjunction with the relevant departments of the State Council; if there are other provisions in laws and regulations, those provisions shall be prevail.

There is no data localization and security assessment on data exports requirement for network operators under effective laws and regulations. Yet the Draft Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft Measures), which was firstly released by the CAC on April 11, 2017 for public comment and a revised draft has been circulated by CAC on August 10, 2017 has extended the security assessment on data exports to network operators. According to the Draft Measures, security assessment shall be conducted when network operators export personal information and important data abroad. Security assessment shall be conducted by network operators and shall be submitted to relevant government authorities when certain criteria are met, such as

the data export contains or accumulatively contains personal information of more than 500,000 individuals. However, such Draft Measures have not been finalized yet.

Q9 **Exceptions for Transfer to Third Counties**

What are the major exceptions to Q8 above?

No.

Q10 **Data Localization**

Is there any requirement to take custody of P.I. in your country?

Please see Question No. 8.

Q11 **Security Control**

What are the major rules for security control of P.I.

According to the CSL, the major obligations for security protection of P.I. are as follows.

(i) Network operators shall keep the user information they have collected strictly confidential and establish and improve user information protection system;

(ii) Network operators shall take technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent the personal information from being divulged, damaged or lost;

(iii) When the personal information is or might be divulged, damaged or lost, they shall take remedial measures immediately, notify the users in a timely;

(iv) Formulating internal security management system and operating procedures, determining the persons in charge of network security and implementing responsibility for network security protection;

(v) Adopting the technical measures for preventing computer virus and the activities endangering network security such as network attack and network intrusion;

(vi) Adopting the technical measures for monitoring and recording network operation status and the network security incidents and keeping relevant network logs for at least 6 months in accordance with relevant provisions;

(vii) Adopting the measures such as data classification as well as backup and encryption of important data.

Hong Kong

Fairbairn Catley Low & Kong

23/F, Shui On Centre, 6-8 Harbour Road, Hong Kong
Contact partner: Ms. Grace Chu

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. The major legislation in Hong Kong is the Personal Data (Privacy) Ordinance ("PDPO").

(2) The PDPO came into force in 1996 and was amended in 2012.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Under the PDPO, personal data is defined as data (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.

Examples of personal data protected by the PDPO include names, phone numbers, addresses, identity card numbers, photos, medical records and employment records.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

There is no specifically defined concept of "sensitive" personal data under the PDPO. However, the Privacy Commissioner for Personal Data ("the Commissioner") has issued Codes of Practice setting out specific requirements in respect of certain types of personal data such as identity card numbers, personal identifiers and consumer credit data. The Commissioner has also indicated that biometric data should only be collected where it is necessary and with the consent of the data subject.

According to the "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement" published by the Commissioner, guidance is laid down for the handling of rather sensitive personal data. If a data user collects sensitive personal data (health, finance, location, etc.), the data user should explain how it uses, processes, handles and transfers such data. The data user should also make it clear in the Privacy Policy Statement whether data subjects have the choice to have such personal data held by the data user erased and express their choice not to have the data shared or transferred.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) Where personal data is collected from the data subject, all practicable steps shall be taken to ensure that he is informed on or before collecting the data of whether it is obligatory or voluntary for him to supply the data; and the consequences if he fails to supply the data. Data subject must be notified of the purpose, the classes of persons to whom the data may be transferred, and his rights to request access to and correction of the data.

(2) In general, no specific consent is required if personal data is used for the purpose for which the data is collected or for a directly related purpose. If the personal data is used for a new purpose, voluntary and explicit consent is required from the data subject. The data user must also obtain the data subject's consent for use of data for direct marketing purpose.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

As mentioned, consent is required if the personal data is used for a new purpose or for direct marketing purpose.

Q6 **Exceptions for Consent**

What are the major exceptions to Q4 and Q5 above?

The PDPO provides a number of exemptions including but not limited to, personal data held for the purpose of safeguarding Hong Kong's security, defence and international relations, crime prevention or detection; assessment or collection of any tax or duty; prevention of

unlawful or seriously improper conduct, news activities; legal proceedings; due diligence exercises; life-threatening emergency situations etc.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

Yes. As mentioned in Q4(1) above, where personal data is collected from the data subject, all practicable steps shall be taken to ensure that he is informed on or before collecting the data of whether it is obligatory or voluntary for him to supply the data; and the consequences if he fails to supply the data. Data subject must be notified of the purpose, the classes of persons to whom the data may be transferred, and his rights to request access to and correction of the data.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

Section 33(2) of the PDPO specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the conditions mentioned in 8 below is met. However, section 33 is not yet in force. Nevertheless, regardless of when section 33 will take effect, the Commissioner encourages data users to adopt the practices recommended to protect personal data.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

Section 33(2) specifies a number of conditions when personal data may be transferred to a place outside Hong Kong:

(a) The place is specified by the Commissioner that there is in force any law which is substantially similar to, or serves the same purposes as, the PDPO;
(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the PDPO;
(c) The data subject has consented in writing to the transfer;
(d) The data user has reasonable grounds for believing that the transfer is for the avoidance of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject; but if it was practicable, such consent would be

given;

(e) the data falls within one of the exemptions under the PDPO;

(f) The data user has taken all reasonable precautions to ensure that the data will not, in that place, be collected, held or used in any manner which, would be a contravention of a requirement under the PDPO.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

Subject to our comments regarding the restriction on transferring personal data to foreign jurisdictions, there is no specific requirement to store the personal data locally.

Q11 Security Control

What are the major rules for security control of P.I.

According to the “Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner’s perspective”, the Commissioner has published a checklist for data users to ensure compliance with the PDPO:

1. Identify any function or activity involving the collection of personal data
2. Identify the purposes of use of the data. Confirm that collection of personal data is necessary and the means of collection are lawful and fair.
3. Take practicable steps to ensure data accuracy and determine the duration that the collected personal data will be retained before erased.
4. Identify whether the use of personal data fall within the original purpose of collection or its directly related purpose.
5. Take practical steps to ensure that there are in place adequate security measures so that personal data collected are protected from unauthorized or accidental access, erasure or other uses.
6. Have privacy policies and practices in place and make them generally available.
7. Handle the data access requests and data correction requests received properly.
8. Identify whether exemptions under the PDPO are applicable.

Indonesia

Armand Yapsunto Muharamsyah & Partners (AYMP)

Richard Yapsunto
richard@aymp.law

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

Up to date, there is no specific law concerning protection of P.I. The Ministry of Communication and Informatics of the Republic of Indonesia, however, has circulated the draft P.I. protection law since 2015 ("**Draft P.I. Protection Law**"), but there is no update on whether the Draft P.I. Protection Law will be enacted in the near future.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Considering there is no specific law concerning protection of P.I., Indonesian law only acknowledges P.I. in electronic systems particularly. Minister of Communication and Informatics Regulation No. 20 Year 2016 concerning Personal Data Protection in Electronic Systems ("**Minister Regulation No. 20/2016**") defines personal data as certain individual data which confidentiality is preserved, maintained, kept, and protected, while "certain individual data" means any true and real information which is inherent and identifiable, either directly or indirectly, to each individual and which usage is according to the laws and regulations.

Further, according to the Draft P.I. Protection Law, "personal data" means any data about a person which is identified and/or identifiable individually or combined with other information, whether directly or indirectly through an electronic or non-electronic system.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Under current prevailing regulation, there is no such as category. The Draft P.I. Protection Law, however, specifically mentions that sensitive P.I. includes religion, health, physical and mental

conditions, biometric, personal habits, sexual life, political views, criminal records, child data, personal financial data, and other information determined as sensitive P.I. by the laws and regulations.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) Pursuant to Minister Regulation No. 20/2016, a P.I. owner may grant written approval, whether manually or electronically after receiving complete explanation with regards to processing of its P.I.

(2) Pursuant to Article 26 of Law No. 11 Year 2008, as amended by Law No. 19 Year 2016 on Electronic Information and Transactions ("**EIT Law**"), the use of information through electronic media that involves P.I. requires the relevant P.I. owner's consent.

In addition to the above, the Draft P.I. Protection Law also requires consent from data subject to acquire or use P.I.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

Please refer to Q4 above.

Q6 **Exceptions for Consent**

What are the major exceptions to Q4 and Q5 above?

Neither EIT Law, nor the Minister Regulation No. 20/2016 provides any exceptions. On the other hand, the Draft P.I. Protection Law mentions that no consent is required with respect to national security, safety protection of the data subject, fulfilment of rights and obligations in relation to manpower, medical treatment by doctor or other medical staff, law enforcement, implementation of authority given by the laws and regulations, P.I. which has already been in public domain.

Q7 **Information to be Provided**

Is there any requirement to provide information upon acquiring P.I.?

Please refer to Q4(1) above.

Q8 **Transfer to Third Countries**

Is there any restriction to transfer P.I. to a foreign country?

There is a restriction to transfer P.I., unless consent from data subject has been obtained.

Q9 **Exceptions for Transfer to Third Counties**

What are the major exceptions to Q8 above?

No exceptions.

Q10 **Data Localization**

Is there any requirement to take custody of P.I. in your country?

No.

Q11 **Security Control**

What are the major rules for security control of P.I.

Any electronic system organizer or operator is required to conduct protection on personal data in electronic system in the process of (i) data obtainment or collection, (ii) data processing and analyzing, (iii) data storage, (ii) data display, publication, transmission, dissemination, and/or opening access to data, and (iv) data destruction.

In addition, once enacted, the Draft P.I. Protection Law will apply not only to Indonesian citizen but also to foreigners in the territory of the Republic of Indonesia.

Japan

Ushijima & Partners

Hioroyasu Kageshima
hiroyasu.kageshima@ushijima-law.gr.jp
+81-5511-3233

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. "Act on the Protection of Personal Information" (APPI) is the law.

(2) Enforced in 2003 and amended in 2017.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Information relating to a living individual which falls under any of each following items:
(i) those containing a name, date of birth, or other descriptions etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other form that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)))) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual)
(ii) those containing an individual identification code

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Yes. Personal information comprising a principal's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair

discrimination, prejudice or other disadvantages to the principal is designated as "Special care-required personal information."

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) No, except for the designated Special care-required personal information.

(2) No.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

Yes.

Q6 **Exceptions for Consent**

What are the major exceptions to Q4 and Q5 above?

As to Q5, above, any provision based on laws and regulations or cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent, no consent is required.

In addition, in those cases set forth in the following, a person receiving the provision of the said personal data shall not fall under a "third party".

(i) cases in which personal data is provided accompanied by a personal information handling business operator entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose;

(ii) cases in which personal data is provided accompanied by business succession caused by a merger or other reason; or

(iii) cases in which personal data to be jointly utilized by a specified person is provided to the specified person, and when a principal has in advance been informed or a state has been in place where a principal can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation of a person responsible for controlling the said personal data.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

The purpose of usage should be informed or disclosed. When P.I. is acquired directly from the data subject, the purpose of usage should be stated explicitly.
In addition, a personal information handling business operator shall put those matters set forth in the following into a state where a data subject can know (including those cases in which it, at the request of a principal, responds without delay).
(i) the name or appellation of the said personal information handling business operator
(ii) the utilization purpose of all retained personal data
(iii) the procedures for responding to a request from a data subject
(iv) besides those set forth under the preceding three items, those prescribed by cabinet order as a necessary matter to ensure the proper handling of retained personal data

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

Prior consent from the data subject is required.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

In those cases set forth in the following, consent from the data subject is not necessary.
(i) such country is designated as the country which has "equivalent standards" to Japan by the Personal Information Protection Commission ("PPC"); or,
(ii) the recipient of P.I. establishes a system conforming to standards prescribed by rules of PPC. This practically means that transferring party and recipient shall enter into a contract to secure the protection of P.I. equivalent to Japanese law.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

No.

Q11

Security Control

What are the major rules for security control of P.I.

PPC's guideline provides the following measures.

(i) Establishment of Privacy Policy;

(ii) Establishment of the internal rules for handing P.I.;

(iii) Establishment of internal organization to protect P.I.;

(iv) Education of personnel;

(v) Physical measure to protect P.I.; and

(vi) Technological measure to protect P.I.

Malaysia

Lee Hishammuddin Allen & Gledhill

Adlin Abdul Majid
Partner - Technology, Media & Telecommunications
Email: aam@lh-ag.com, Telephone: +603 6208 5816

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. The main law on personal data protection is the "Personal Data Protection Act 2010" ("PDPA").
(2) The PDPA was enforced on 15 November 2013 and has not been amended as at the date of writing.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

The PDPA governs the processing of "personal data". Personal data is defined as any information in respect of commercial transactions, which:
(i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
(ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
(iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Yes. Sensitive personal data is defined to mean any personal data consisting of information as to the physical or mental health or condition of a data subject; his political opinions; his religious beliefs or other beliefs of a similar nature; the commission or alleged commission by him of

any offence; or any other personal data as the Minister charged with the responsibility for the protection of personal data (currently the Minister of Communications and Multimedia) ("Minister") may determine.

Q4	**Consent for Acquisition or Usage** (1) Is consent from the data subject required to acquire P.I.? (2) Is consent from the data subject required to use P.I.?

(1) Yes.

(2) Yes.

Q5	**Consent for Provision** Is consent from the data subject required to provide P.I. to a third party?

Yes.

Q6	**Exceptions for Consent** What are the major exceptions to Q4 and Q5 above?

With regard to Q4 above, consent is not required if the processing of the personal data is necessary:
(i) for the performance of a contract to which the data subject is a party;
(ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
(iii) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
(iv) in order to protect the vital interests of the data subject;
(v) for the administration of justice; or
(vi) for the exercise of any functions conferred on any person by or under any law.

Note that explicit consent is required for the processing of sensitive personal data, and sensitive personal data may be processed without explicit consent if the processing of personal complies with specific conditions, including where the processing is for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the

data user in connection with employment; in order to protect the vital interests of the data subject; for medical purposes; and for the purpose of, or in connection with, any legal proceedings.

With regard to Q5 above, personal data may be disclosed to third parties without consent of the data subject, if it is disclosed for a purpose for which the personal data was to be disclosed at the time of collection, or for any directly related purpose; or if it is disclosed to a class of third parties set out in a written notice issued pursuant to the Notice and Choice Principle (see Q7, below). Further, disclosure can be made without consent in certain necessary circumstances, including for the purpose of preventing or detecting a crime, or for the purpose of investigations; or where disclosure is required or authorised by or under any law or by the order of a court.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

The Notice and Choice Principle requires a data user to give data subjects written notice on the processing of the data subjects' personal data by the data user. This notice must contain specific information, including the description of the personal data being processed; the purposes for which the personal data is collected and further processed; and the class of third parties to whom the data user may disclose the personal data.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

Yes. Data users cannot transfer a data subject's personal data to a location outside Malaysia unless it is to a location specified by the Minister. At the moment, no locations have been specified.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

The major exceptions include where the data subject consents to the transfer; where the transfer is necessary for the conclusion or performance of a contract; where the transfer is for the purpose of any legal proceedings, for obtaining legal advice or establishing, exercising or defending legal right; and where the data user takes all reasonable precautions and exercises

all due diligence to ensure that the transferred personal data will not, in the place of transferred, be processed in any manner that contravenes the PDPA.

Q10	**Data Localization** Is there any requirement to take custody of P.I. in your country?

No.

Q11	**Security Control** What are the major rules for security control of P.I.

Data users must take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

The Personal Data Protection Standards 2015, issued pursuant to the PDPA, establish specific security standards for electronically and non-electronically processed personal data, including imposing requirements on a data user to control, limit and regulate employees' access to personal data systems; to safeguard computer systems from malware threats and regularly update back up or recovery systems and anti-virus; to regulate the use of removable devices and cloud computing services; and to enter into a binding contract with any third party processing personal data on behalf of the data user, to ensure compliance with safety requirements.

New Zealand

Lowndes Ltd

Mark Lowndes
Director
mark.lowndes@lowndeslaw.com
DDI: +64 9 373 7286 M: +64 21 921 323
Kerri Dewe
Principal
kerri.dewe@lowndeslaw.com
DDI: +64 9 373 7280 M: +64 21 537 747

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. The Privacy Act 1993.

(2) The Act came into force on 1 July 1993.
Almost every person or organization that collects or holds P.I. is an “Agency” and subject to the requirements of the Privacy Act. This includes individuals, companies, government departments, religious groups, schools, clubs and so on.

Q2 Definition of “Personal Information”

In the law mentioned in Q1 above, what information is designated as P.I.?

P.I. is information about an identifiable individual, being a natural person, other than a deceased natural person. New Zealand’s Privacy Commissioner has commented that “Personal information is any piece of information that relates to a living, identifiable human being. People's names, contact details, financial health, purchase records: anything that you can look at and say "this is about an identifiable person". Even if their name doesn't appear, it could be personal information. The question is whether there's a reasonable chance that someone could be identified from the information. Also, it does not need to be "secret" or "sensitive" - it just needs to be about them.”
P.I. is not:
- information about a company or organisation;
- information that is not capable of identifying an individual;

- information about deceased individuals (subject to limited exceptions).

Q3 **Special Categories of Personal Information (Sensitive Information, etc.)**

Is there any special category of P.I. such as sensitive information?

No. The Privacy Act does not specify categories of "sensitive" information or data subject to special controls.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) In general, an Agency should collect P.I. directly from the data subject. However, see the exceptions discussed below.

(2) No, provided that it is being used for the purposes for which it was collected. However, see the exceptions discussed below.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

No, provided that it is being disclosed for the purposes for which it was collected. However, see the exceptions discussed below.

Q6 **Exceptions for Consent**

What are the major exceptions to Q4 and Q5 above?

(i) An Agency can collect P.I. from other sources, without consent from the data subject, in prescribed situations:

a. Where the P.I. is publicly accessible;
b. Where collection from another source would not prejudice the interests of the data subject;
c. Where collection from the data subject would prejudice the purposes of the collection;
d. Where collection from the data subject is not reasonably practicable in the

circumstances of the particular case; or

e. Where the P.I. will not be used in a form in which the data subject is identified (e.g. for statistical or research purposes); and
f. For law enforcement purposes.

(ii) An Agency can use P.I. without consent and contrary to the purpose for which it was collected in prescribed situations:

a. The purpose for which the P.I. is used is directly related to the purpose in connection with which the P.I. was obtained;
b. The P.I. is publicly available and that, in the circumstances of the case, it would not be unfair or unreasonable to use the P.I.;
c. It is necessary to prevent or lessen a serious threat to the public or an individual;
d. The P.I. will not be used in a form in which the data subject is identified (e.g. for statistical or research purposes); or
e. The P.I. is used for law enforcement purposes.

(iii) An Agency can disclose P.I. to a third party without consent and contrary to the purpose for which it was collected in prescribed situations:

a. The P.I. is publicly available and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the P.I.;
b. It is necessary to prevent or lessen a serious threat to the public or an individual;
c. The P.I. will not be used in a form in which the data subject is identified (e.g. for statistical or research purposes);
d. The disclosure of the P.I. is necessary to facilitate the sale or other disposition of a business as a going concern; or
e. The P.I. is used for law enforcement purposes.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

When collecting P.I. directly from the data subject, the Agency must take any steps that are, in the circumstances, reasonable to ensure that the data subject is aware of:

(i) The fact the P.I. is being collected;
(ii) The purpose for which the P.I. is being collected;
(iii) The intended recipients of the P.I.;
(iv) The name and address of the Agency collecting the P.I. and holding the P.I.;
(v) If the collection of the P.I. is authorised or required by or under law:

a. The particular law by or under which the collection of the P.I. is so authorised or required; and

b. Whether or not the supply of the P.I. by the data subject is voluntary or mandatory;

(vi) The consequences (if any) for the data subject if all or any part of the requested P.I. is not provided; and

(vii) The rights of access to, and correction of, P.I. provided by the Privacy Act.

It is not necessary for an Agency to comply with these requirements if the Agency believes, on reasonable grounds that:

(i) Non-compliance is authorised by the data subject;

(ii) Non-compliance would not prejudice the interests of the data subject;

(iii) Compliance would prejudice the purposes of the collection;

(iv) Compliance is not reasonably practicable in the circumstances of the particular case; or

(v) The P.I. will not be used in a form in which the data subject is identified (e.g. for statistical or research purposes); and

(vi) The P.I. will be used for law enforcement purposes.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

The Privacy Commissioner may prohibit a transfer of P.I. from New Zealand to another country if the Commissioner is satisfied, on reasonable grounds, that:

(i) The P.I. has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to the Privacy Act; and

(ii) The transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

The restrictions above do not apply if the transfer of the P.I., or the P.I. itself, is:

(i) Required or authorised by or under any legislation; or

(ii) Required by any convention or other instrument imposing international obligations on New Zealand.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

No. Subject to our comments regarding the restriction on transferring P.I. to a foreign country, there is no requirement to store P.I. domestically.

Q11	**Security Control** What are the major rules for security control of P.I.

The Privacy Act requires that where an Agency holds P.I. they must ensure that:

(i) The P.I. is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss or unauthorised use; and

(ii) If it is necessary for the P.I. to be given to a person in connection with the provision of a service to the Agency, everything reasonably within the power of the Agency is done to prevent unauthorised use or unauthorised disclosure of the P.I..

Pakistan

Meer & Hasan

306-Al-Faisal Plaza, 48-The Mall Road, Lahore-54000,
Pakistan.
Tel: +92-42-37235812, Fax: +92-42-37234332
E-mail: mail@meerhasan.com
Website: www.meerhasan.com

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) No

(2) N/A

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

N/A

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

N/A

Q4 Consent for Acquisition or Usage

(1) Is consent from the data subject required to acquire P.I.?
(2) Is consent from the data subject required to use P.I.?

(1) Not required but is advisable to do so.

(2) Not required but is advisable to do so.

Q5	**Consent for Provision** Is consent from the data subject required to provide P.I. to a third party?

Not required but is advisable to do so.

Q6	**Exceptions for Consent** What are the major exceptions to Q4 and Q5 above?

N/A

Q7	**Information to be Provided** Is there any requirement to provide information upon acquiring P.I.?

No.

Q8	**Transfer to Third Countries** Is there any restriction to transfer P.I. to a foreign country?

No.

Q9	**Exceptions for Transfer to Third Counties** What are the major exceptions to Q8 above?

N/A

Q10	**Data Localization** Is there any requirement to take custody of P.I. in your country?

No.

Q11

Security Control

What are the major rules for security control of P.I.

None, however, a reasonable standard of care should be exercised.

Philippines

SyCip Salazar Hernandez & Gatmaitan

Address: SyCipLaw Center, 105 Paseo de Roxas, Makati City, Philippines, 1226

Carina C. Laforteza cclaforteza@syciplaw.com
Eugenio M. Leynes emleynes@sycipalw.com

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) The Philippines' data protection law is Republic Act No. 10173 or the "Data Privacy Act of 2012" ("**DPA**"). The DPA mandated the creation of a National Privacy Commission ("**NPC**") to implement, enforce, and monitor compliance of covered entities with the DPA. Pursuant to the mandate, the NPC promulgated the implementing rules and regulations of the DPA ("**IRR**"). The NPC also issues Circulars, Advisories and Advisory Opinions to clarify and implement the various provisions of the DPA.

(2) The DPA took effect on September 8, 2012. Following a period of public consultation, the NPC finalized and formally promulgated the IRR on August 24, 2016, and came into effect on September 9, 2016.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

The DPA defines the term "personal data" as referring to "all types of personal information," which covers any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

Q3 **Special Categories of Personal Information (Sensitive Information, etc.)**

Is there any special category of P.I. such as sensitive information?

The DPA defines a sub-category of personal information as "sensitive personal information," which covers any personal information:

i. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
ii. about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
iii. issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
iv. specifically established by an executive order or a law to be kept classified.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?
(2) Is consent from the data subject required to use P.I.?

(1) The DPA expressly requires that in order to first collate, process, and then use or share, personal data, the personal information controller or processor must have a lawful criterion or basis for processing, such as consent.

(2) Please see response to Q4(1) above.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

Please see response to Q4(1) above.

The DPA differentiates the transfer of personal information to a third party pursuant to (1) a data sharing arrangement and (2) an outsourcing agreement.

Data sharing is defined as the disclosure or transfer to a third party of personal data under the

custody of a personal information controller or personal information processor. It contemplates that the purpose of the processing by the third-party is different from that of the personal information controller. This will require the separate consent of the data subject, agreeing to the sharing of data.

On the other hand, an outsourcing agreement pertains to the disclosure or transfer of personal data by the personal information controller to a personal information processor in order for the latter to perform the particular activities outsourced by the former. In such an arrangement, the personal information controller need not obtain the separate consent of the data subject to transfer his or her personal information. The original consent to process his or her personal information will suffice.

Q6 Exceptions for Consent

What are the major exceptions to Q4 and Q5 above?

The following are instances when other criteria for lawful processing are present and the processing of personal information is allowed even without consent:

- The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;
- The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;
- The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;
- The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or
- The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.

However, these other instances are construed strictly against the controller or processor.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling. Prior to collection and processing of personal data, the data subject must be informed of the following:

i. The fact of collection and processing of personal data pertaining to the data subject;
ii. Description and categories of personal data being collected and processed;
iii. Purpose for the collection, and processing, including the purposes for data sharing or automated processing;
iv. Lawful basis of the collection and processing, when the data subject has not given consent;
v. Scope and method of personal data processing;
vi. Identities of intended recipients of personal data;
vii. Methods and logic used for automated processing, if any;
viii. Identity and contact details of the personal data controller or its representative;
ix. Retention period; and
x. Rights of a data subject.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

The DPA does not impose restrictions on the transfer of personal data to a foreign country. However, the personal information controller would continue to be responsible for any personal data transferred internationally.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

N/A

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

There is no requirement under the DPA to keep the personal data in the Philippines. However, the personal information controller would continue to be responsible for any personal data transferred internationally.

Q11 Security Control

What are the major rules for security control of P.I.

Controllers and processors are required to implement appropriate organizational, physical, and technical security measures intended for the protection of personal data against any unlawful processing.

Organizational security measures include:

- Creation and implementation of a data protection policy/manual;[1]
- Management of human resources – non-disclosure agreements, training, and capacity building; and
- Regular review and monitoring of privacy and security policies

Physical security measures include:

- Design of office space and work stations, including the physical arrangement of furniture and equipment that ensure privacy; and
- Limiting access to records and work stations

Technical security measures include:

- Security policy system monitoring; and
- Encryption and authentication process

[1] The Privacy Manual is an internal document, which according to the NPC, must contain the following:

- An overview of the Data Privacy Act, its implementing rules and regulations, and other policies and issuances that relate to data protection and which are relevant to the industry or sector of the company, including the transactions it regularly carries out;
- Scope and limitations;
- Records of processing activities –
  - Purpose of processing;
  - Data subjects and type of data;
  - Data flow;
  - Security measures;
  - Contact persons
- Procedure for collection, use or disclosure, storage, and disposal of personal data;
- Access management and system monitoring;
- Protocols to follow during security incidents or technical problems and breach management;
- Policies and procedure for data subjects to exercise their rights under the DPA;
- Regular review and monitoring of privacy and security policies

Singapore

Donaldson & Burkinshaw LLP

Tel: +65 6533 9422; Fax: +65 6533 7806
chiduan.gooi@donburk.com.sg
enquiries@donburk.com.sg

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. The "Personal Data Protection Act 2012 (No. 26 of 2012)" ("**PDPA**").

(2) The PDPA commenced on 2 January 2013 where provisions on the formation of the Personal Data Protection Commission ("**PDPC**") came into force. Provisions relating to the Do Not Call ("**DNC**") Registry came into effect on 2 January 2014 and the main sections relating to, inter alia, collection and use of personal data only came into effect on 2 July 2014.
The latest amendment was made on 1 October 2016.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Under Section 2 of the PDPA, "personal data" means data, whether true or not, about an individual who can be identified –

(a) From that data; or
(b) From that data and other information to which the organisation has or is likely to have access.

The PDPA does not apply to:

(a) personal data about an individual that is contained in a record that has been in existence for at least 100 years; or
(b) personal data about a deceased individual, with the exception that the provisions on the disclosure and protection of personal data applies to an individual who has been dead for 10 years or fewer.

The PDPA also does not apply to business contact information, defined as an individual's name, position name or title, business telephone number, business address, business electronic mail

address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

It is intended that from 1 September 2019, organisations will generally not be allowed to collect, use or disclose NRIC numbers/copies of NRIC unless such collection, use or disclosure is required under the law or required to accurately establish or verify the identities of the individuals to a high degree of fidelity.

The Singapore National Registration Identity Card ("NRIC") number is a unique identifier assigned by the Singapore Government to her citizens and permanent residents and it is often used in transactions with the Government as well as in commercial transactions. The NRIC also contains the name, photo, address, date of birth and race of the holder.

Q4 Consent for Acquisition or Usage

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) Yes. Section 13 of the PDPA prohibits organisations from **collecting** personal data about an individual unless —

a) the individual gives, or is deemed to have given, his consent under the PDPA to the collection; or
b) the collection without the consent of the individual is required or authorised under the PDPA or any other written law.

(2) Yes. Section 13 of the PDPA prohibits organisations from **using** personal data about an individual unless —

a) the individual gives, or is deemed to have given, his consent under the PDPA to the use; or
b) the use without the consent of the individual is required or authorised under the PDPA or any other written law.

Q5 Consent for Provision

Is consent from the data subject required to provide P.I. to a third party?

Yes. Section 13 of the PDPA prohibits organisations from **disclosing** personal data about an individual unless —

a) the individual gives, or is deemed to have given, his consent under the PDPA to the disclosure; or
b) the disclosure without the consent of the individual is required or authorised under the PDPA or any other written law.

Q6 Exceptions for Consent

What are the major exceptions to Q4 and Q5 above?

Section 17 of the PDPA allows for the collection, use, and/or disclosure of personal data without consent subject to the circumstances and conditions in the Second, Third, and Fourth Schedule of the PDPA respectively.

In particular, an organisation may collect, use, and/or disclose personal data about an individual without the consent of the individual or from a source other than the individual in any of the following circumstances:

a) the collection, use, and/or disclosure is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection, use, and/or disclosure cannot be obtained in a timely way;
b) the collection, use, and/or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;
c) the personal data is publicly available;
d) the collection, use, and/or disclosure is necessary in the national interest;
e) the collection, use, and/or disclosure is necessary for any investigation or proceedings;
f) the collection, use, and/or disclosure is necessary for evaluative purposes;
g) the personal data is collected, used, and/or disclosed for the organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation; or
h) the collection, use, and/or disclosure is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

Yes. Under Section 20 of the PDPA, an organisation must inform or notify the individual the purpose for use or disclosure of his personal data, on or before collecting the personal data. Section 20(1) states that an organisation shall inform the individual of —

a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data;
b) *any other purpose* of the use or disclosure of the personal data of which the individual has not been informed under paragraph (*a*), before the use or disclosure of the personal data for that purpose; and
c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

Yes. Section 26(1) of the PDPA prohibits an organization from transferring any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

Regulation 9 of the Personal Data Protection Regulations 2014 stipulates the requirements for the transfer of personal data under Section 26 of the PDPA:

9.— (1) For the purposes of section 26 of the Act, a transferring organisation must, before transferring an individual's personal data to a country or territory outside Singapore —

a) take appropriate steps to ensure that the transferring organisation will comply with Parts III to VI of the Act, in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation; and
b) take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data in that country or territory outside Singapore (if any) is bound by legally enforceable obligations (in accordance with regulation 10) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act.

(2) A transferring organisation is taken to have satisfied the requirements of

paragraph (1)(a) in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation if the personal data is —

a) data in transit; or

b) publicly available in Singapore.

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

a) subject to paragraph (4), the individual consents to the transfer of the personal data to that recipient in that country or territory;

b) the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation;

c) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party which is entered into at the individual's request;

d) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party if a reasonable person would consider the contract to be in the individual's interest;

e) the transfer of the personal data to the recipient is necessary for the personal data to be used under paragraph 1(a), (b) or (d) of the Third Schedule to the Act or disclosed under paragraph 1(a), (b), (c), (e) or (o) of the Fourth Schedule to the Act, and the transferring organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose;

f) the personal data is data in transit; or

g) the personal data is publicly available in Singapore.

(4) An individual is not taken to have consented to the transfer of the individual's personal data to a country or territory outside Singapore if —

a) the individual was not, before giving his consent, given a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act;

b) the transferring organisation required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; or

c) the transferring organisation obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices.

(5) An individual may withdraw any consent given for the transfer of the personal data to a

country or territory outside Singapore.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

Section 26(2) is an exception to Section 26(1), which provides that the PDPC may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to Section 26(1) in respect of any transfer of personal data by that organisation.

The Fourth Schedule to the PDPA provides the situations whereby disclosure can be made without obtaining and exemption or consent:

1. An organisation may disclose personal data about an individual without the consent of the individual in any of the following circumstances:
   a) the disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way;
   b) the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;
   c) subject to the conditions in paragraph 2, there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way;
   d) the personal data is publicly available;
   e) the disclosure is necessary in the national interest;
   f) the disclosure is necessary for any investigation or proceedings;
   g) the disclosure is to a public agency and such disclosure is necessary in the public interest;
   h) the disclosure is necessary for evaluative purposes;
   i) the disclosure is necessary for the organisation to recover a debt owed by the individual to the organisation or for the organisation to pay to the individual a debt owed by the organisation;
   j) the disclosure is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;
   k) the personal data is disclosed by a member of a credit bureau to the credit bureau for the purpose of preparing credit reports, or in a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual;
   l) the personal data about the current or former students of the organisation, being an

education institution, is disclosed to a public agency for the purposes of policy formulation or review;

m) the personal data about the current or former patients of a healthcare institution licensed under the Private Hospitals and Medical Clinics Act (Cap. 248) or any other prescribed healthcare body is disclosed to a public agency for the purposes of policy formulation or review;

n) the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer;

o) the disclosure is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual;

p) subject to the conditions in paragraph 3, the personal data —

   i. is disclosed to a party or a prospective party to a business asset transaction with the organisation;

   ii. is about an employee, customer, director, officer or shareholder of the organisation; and;

   iii. relates directly to the part of the organisation or its business assets with which the business asset transaction is concerned;

q) subject to the conditions in paragraph 4, the disclosure is for a research purpose, including historical or statistical research;

r) the disclosure is for archival or historical purposes if a reasonable person would not consider the personal data to be too sensitive to the individual to be disclosed at the proposed time; or

s) subject to the conditions in paragraph 5, the personal data —

   i. was collected by the organisation in accordance with Section 17(1); and

   ii. is disclosed by the organisation for purposes consistent with the purpose of that collection.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

No, there is no requirement to take custody of personal data in Singapore.

However, pursuant to Section 24 of the PDPA, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or

similar risks.

Q11	**Security Control** What are the major rules for security control of P.I.

Broadly, the PDPA has 9 main obligations which organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data, namely:

(1) Consent Obligation: To obtain individual's consent before collecting, using or disclosing his personal data for a purpose.

(2) Purpose Limitation Obligation: To collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

(3) Notification Obligation: To notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.

(4) Access and Correction Obligation: Upon request, (i) provide an individual with his/her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data.

(5) Accuracy Obligation: Make reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation.

(6) Protection Obligation: To protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

(7) Retention Limitation Obligation: To cease to retain documents containing personal data or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (ii) retention is no longer necessary for legal or business purposes.

(8) Transfer Limitation Obligation: Not to transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

(9) Openness Obligation: To implement the necessary policies and procedures in order to meet its obligations under the PDPA and make information about its policies and procedures publicly available.

South Korea

Lee & Ko

Kwang Bae Park kwangbae.park@leeko.com
Sunghee Chae sunghee.chae@leeko.com

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. The "Personal Information Protection Act" (PIPA) is the law. Additionally, there are various sector-specific laws which also regulate the handling of P.I. such as the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. and the Credit Information Use and Protection Act. In this article, we will focus on the PIPA as it is the general law on data protection.

(2) The PIPA entered into effect in 2011 and was most recently amended in 2017.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

Under the PIPA, P.I. is defined as "any information relating to an individual living person from which such individual can be identified through one's name, resident registration number, or visual image, etc. (including any information from which, if not by itself, but can be easily combined with other information, to identify a specific individual)."

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Yes. Under the PIPA, P.I. comprising a data subject's ideology, creed, membership of a labor union or political party, political views, health, sexual preferences, bio-data, criminal records, or any other information which, if divulged, may considerably infringe upon such data subject's privacy is defined as "sensitive information". In addition, P.I. comprising unique identifiers which are assigned to each individual such as resident registration numbers, passport numbers, driver's license numbers, and alien registration numbers are defined as "particular identification information".

Q4	**Consent for Acquisition or Usage** (1) Is consent from the data subject required to acquire P.I.? (2) Is consent from the data subject required to use P.I.?

(1) Yes.

(2) Yes.

Q5	**Consent for Provision** Is consent from the data subject required to provide P.I. to a third party?

Yes.

Q6	**Exceptions for Consent** What are the major exceptions to Q4 and Q5 above?

(i) P.I. may be collected/used without the data subject's consent in cases where:

- collection/use is specifically required or permissible under other applicable laws and regulations, or necessary to comply with the data handler's obligations under other applicable laws and regulations;
- collection/use is necessary to enter into and perform a contract with the data subject;
- there exists a clear and urgent need to protect the life, physical or economic interest of the data subject or a third party, and the consent to the collection/use of P.I. cannot be obtained in an ordinary manner because the data subject (or his/her legal guardian) cannot express his/her intent, or his/her address is unknown; or
- collection/use is necessary to achieve a legitimate interest of the data handler where such interest clearly overrides the rights of the data subject; provided that the collection/use will be substantially relevant to the legitimate interest of the data handler, and that such collection/use is performed only to a reasonable extent.

(ii) P.I. may be provided to third parties without the data subject's consent in cases where:

- provision is specifically required or permissible under other applicable laws and regulations, or necessary to comply with the data handler's obligations under other applicable laws and regulations; or

- there exists a clear and urgent need to protect the life, physical or economic interest of the data subject or a third party, and the consent to the provision of P.I. cannot be obtained in an ordinary manner because the data subject (or his/her legal guardian) cannot express his/her intent, or his/her address is unknown.

In addition, separate exceptions may be applicable for each special category of personal information, which we do not elaborate here for the for the sake of conciseness.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

When obtaining consent for the collection/use of P.I., data subjects must be provided notice of the following information:

- purpose for collecting/using P.I.;
- items of P.I. to be collected;
- periods of use/retention for the P.I.; and

disadvantages that the data subject will face in case he/she refuses to provide consent.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

The PIPA provides separate requirements for the provision of P.I. (Provision) and the outsourcing of the processing of P.I. (Outsourcing). Specifically, a Provision refers to cases where a data transfer is conducted for the benefit and business purpose of the transferee whereas an Outsourcing refers to cases where a data transfer is conducted for the benefit and business purpose of the transferor. If a data controller conducts a Provision to a third party in a foreign country, it is required to obtain the consent of data subjects after providing notice of certain matters prescribed by law. In contrast, if a data controller conducts an Outsourcing to a third party in a foreign country, the data controller is not required to obtain such consent. However, data handlers are required to indicate the specific tasks to be outsourced and the name(s) of the outsourced processor(s) in their privacy policy so that such information is readily available to data subjects.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

Please refer to our responses for Q5 above regarding the cases where P.I. may be provided to third parties without the data subject's consent.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

In principle, the PIPA and other data protection laws in Korea do not prescribe any data localisation requirements. However, according to regulations in the financial and medical sectors, certain data, including P.I., is required to be physically stored in Korea and it is prohibited to transfer copies of such data abroad.

Q11 Security Control

What are the major rules for security control of P.I.

The PIPA sets forth very specific security requirements with regard to the security of P.I.
For instance, the PIPA (and its Enforcement Decree) requires data handlers to implement certain managerial, technical, and physical safety measures such as the following in order to prevent the loss, theft, leakage, falsification, alteration or damage of personal data:

- Establish and implement an internal administrative plan for the safe processing of P.I.;
- Implement measures to place restrictions on the access to P.I. and access authority;
- Apply encryption technology to P.I. or take other equivalent measures to ensure the secure storage and transmission of P.I.;
- Maintain access logs/records and take measures to prevent forging or falsification of such records, in order to be able to effectively respond to an intrusion incident;
- Install and update security programs for the protection of P.I.;
- Implement physical measures such as setting up separate storage facilities for securely storing P.I.

The Standards of Personal Information Protection Measures, an implementing regulation of the PIPA, provides detailed information on security measures that must be implemented.

Sri Lanka

VARNERS

Level 14, West Tower, World Trade Center
Echelon Square, Colombo 01, SRI LANKA
TEL: (+94 11) 2394350 -1 (+94 11) 5544711
FAX: (+94 11) 2394353 (+94 11) 5529429

Q1 **Legal System**

(1) Is there a specific law concerning the protection of personal information (P.I.)?

(2) What is the effective and/or amended date of such law?

(1) Sri Lanka does not have any statues concerning the protection of personal information.

(2) N/A

Q2 **Definition of "Personal Information"**

In the law mentioned in Q1 above, what information is designated as P.I.?

N/A

Q3 **Special Categories of Personal Information (Sensitive Information, etc.)**

Is there any special category of P.I. such as sensitive information?

No.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

No.

Q5	**Consent for Provision** Is consent from the data subject required to provide P.I. to a third party?

No.

Q6	**Exceptions for Consent** What are the major exceptions to Q4 and Q5 above?

If there is a private contract between the parties relating to acquisition and usage of P.I. or sharing thereof, then such acquisition, usage or sharing of P.I. will be subject to the terms of such contract.

Q7	**Information to be Provided** Is there any requirement to provide information upon acquiring P.I.?

No. If there is a private contract between the parties then this will be subject to the terms of such contract.

Q8	**Transfer to Third Countries** Is there any restriction to transfer P.I. to a foreign country?

No.

Q9	**Exceptions for Transfer to Third Counties** What are the major exceptions to Q8 above?

If there is a private contract between the parties then this will be subject to the terms of such contract.

Q10	**Data Localization** Is there any requirement to take custody of P.I. in your country?

No.

Q11

Security Control

What are the major rules for security control of P.I.

Statute has not prescribed any such rules for security control of P.I. in Sri Lanka.

If there is a private contract between the parties then this will be subject to the terms of such contract.

Taiwan

Lee and Li, Attorneys at Law

Benjamin Li (Partner): benjaminli@leeandli.com
David Tien (Senior Associate): davidjtien@leeandli.com

Q1 Legal System

(1) Is there a specific law concerning the protection of personal information (P.I.)?
(2) What is the effective and/or amended date of such law?

(1) Yes. The Personal Data Protection Act ("PDPA") is the law regulating the collection, processing, use and transfer of personal data in Taiwan.

(2) Enforced in 2012 and amended in 2016.

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

The PDPA defines "personal data" as a natural person's name, date of birth, national identification number, passport number, physical appearance, fingerprint, marital status, family background, educational background, occupation, medical history, medical treatments, genetic data, sex life, health check results, criminal record, contact information, financial condition, social activities and any other information that may be used to directly or indirectly identify a natural person.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

Yes. Under the PDPA, "sensitive data" includes personal data with regard to medical history, medical treatments, genealogy, sex life, health-check results and criminal records.

Q4 Consent for Acquisition or Usage

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) Under the PDPA, a non-government agency may collect and process personal data only if (i) the personal data is necessary for serving one or more specified and lawful purposes, and (ii) such collection is based on a statutory ground (such as informed consent having been granted by the data subject, or a contractual or quasi-contractual relationship with the data subject). If the non-government agency collects personal data based on a contractual or quasi-contractual relationship with the data subject, consent from the data subject is not required.

(2) Under the PDPA, a non-government agency may use the personal data collected (including sending marketing communications, providing a third party with the personal data, etc.) so long as such use does not go beyond the necessary extent in relation to the purposes for which the non-government agency collects the personal data. Under the circumstance where the use of the personal data collected does not go beyond the necessary extent in relation to the purposes for such collection, consent from the data subject is not required. However, if the non-government agency use the personal data for any new purpose(s) rather than the original purpose(s) for which the personal data is collected, an additional statutory ground would be required, such as informed consent having been granted by the data subject.

Q5 Consent for Provision

Is consent from the data subject required to provide P.I. to a third party?

Providing a third party with personal data would be deemed as the use of personal data under the PDPA. Therefore, our response to Question 4(2) above would apply in the scenario where the entity collecting the personal data wishes to transfer it to a third party.

Q6 Exceptions for Consent

What are the major exceptions to Q4 and Q5 above?

A non-government agency may collect personal data based on a contractual or quasi-contractual relationship with the data subject. Also, in addition to obtaining informed consent from the data subject, a non-government agency may use the personal data collected for a new purpose if such use is required by law.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

Yes. Under the PDPA, a non-government agency must inform the data subject of the following information at the time of collection: (i) the identity of the data collector; (ii) the purpose(s) for which his/her data is collected; (iii) the type of personal data collected; (iv) the term, place and method of use and the persons who may use the data; (v) the data subject's rights in relation to his/her personal data under the PDPA; and (vi) the consequences of his/her failure to provide the requested personal data.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

The PDPA authorizes central competent authorities to impose restrictions on cross-border transfer of personal data if:

(i) the transfer would prejudice any material national interest;
(ii) the transfer is prohibited or restricted under an international treaty or agreement;
(iii) the country to which the personal data are to be transferred does not afford sound legal protection of personal data, thereby affecting the interests of the data subjects; or
(iv) the purpose of the transfer is to evade the restrictions under the PDPA.

On 25 September 2012, the National Communications Commission issued a blanket order prohibiting communications enterprises from transferring subscribers' personal data to the People's Republic of China (the "PRC") on the grounds that the personal data protection laws in the PRC are still inadequate. Based on the public information available thus far, no other competent authority has issued any other order prohibiting a non-government agency from transferring personal data outside of Taiwan.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

N/A

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

No.

Q11 Security Control

What are the major rules for security control of P.I.

The PDPA only requires a non-government agency to have in place appropriate measures to prevent personal data from being stolen, altered, damaged, destroyed, lost or disclosed.

The Enforcement Rules of the PDPA further provide certain technical and organizational measures that a non-government agency may consider adopting based on the principle of proportionality, i.e., based on the quality and quantity of the personal data involved, including but not limited to the following:

1. allocation of personnel to enforce the measures and sufficient resources;
2. identification of the scope of personal data;
3. personal data risk assessment and the management mechanism thereof;
4. mechanism for prevention, notification, and handling of incident;
5. internal management procedures for collection, processing, and use of personal data;
6. data security management and personnel management;
7. awareness programs and training;
8. facility security management;
9. data security auditing mechanism;
10. maintenance of access records, track log files, and relevant evidence; and
11. continuous improvement on security and maintenance measures.

Thailand

Tilleke & Gibbins

Athistha (Nop) Chitranukroh
email: athistha.c@tilleke.com

Q1	**Legal System** (1) Is there a specific law concerning the protection of personal information (P.I.)? (2) What is the effective and/or amended date of such law?

No. Currently, Thailand does not have unified comprehensive privacy legislation.

However, currently, there is a draft personal data protection act (Data Privacy Bill – "**Bill**"), which has been published by the Council of State and approved in principle by the Thai Cabinet (in 2015). It was circulated for a 4th public hearing in January 2018, and it is anticipated that the draft will be enacted in early 2019. The Draft Privacy Bill, once implemented, will generally require the following:

- The establishment of the Office of Personal Data Protection Commission ("**Commission**");
- Consent for collection, use, and transfer of personal data must be obtained from the data owner in writing, or by electronic means;
- When obtaining consent, specific purposes of the collection, use, and transfer must be clearly communicated to the data owner;
- Data controllers, once they have obtained the personal data, must put in place a secure system for storing the data, in order to prevent unauthorized access to the data; and;
- The law, once enacted, will provide a grace period of 365 days.

Presently, the legal protection of privacy is recognized under the Constitution of the Kingdom of Thailand, which is the supreme law. In the absence of unified comprehensive privacy legislation, Thailand's personal data protection law regime is industry-specific, with certain sectors, such as telecommunications, banking, securities, consumer credit, and electronic payment services, all having separate approaches to personal data protection.

Q2 **Definition of "Personal Information"**

In the law mentioned in Q1 above, what information is designated as P.I.?

Currently not defined under Thai law.

According to the Bill, "**Personal Data**" means any data pertaining to a person, including a deceased person, which enables the identification of such person, whether directly or indirectly, but not including data which specifies only the name, title, work place, or business address.

Q3 **Special Categories of Personal Information (Sensitive Information, etc.)**

Is there any special category of P.I. such as sensitive information?

No, under the present law and according to the Bill.

Q4 **Consent for Acquisition or Usage**

(1) Is consent from the data subject required to acquire P.I.?

(2) Is consent from the data subject required to use P.I.?

(1) No, under the present law. Yes, according to the Bill.

(2) No, under the present law. Yes, according to the Bill except fall within the prescribed exemptions.

Q5 **Consent for Provision**

Is consent from the data subject required to provide P.I. to a third party?

No, under the present law. Yes, according to the Bill.

Q6 **Exceptions for Consent**

What are the major exceptions to Q4 and Q5 above?

Not applicable under the present law.

Under the Bill, consent is required unless:

(i) it is for the interests of education, research or statistics, and such Personal Data is kept confidential;
(ii) it is for preventing or suppressing a danger to a person's life, body or health;
(iii) it is information that is disclosed to the public with the direct, or implied, consent of the Data Subject;
(iv) it is an act that is in compliance with the law; or
(v) it is as otherwise prescribed by the Commission.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

No, under the present law. Yes, according to the Bill.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

No, under the present law.

Under the Bill, it is not a prohibition but subject to certain requirements.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

Not applicable under the present law.

Under the Bill, the overseas transfer of Personal Data must be made in accordance with a specific regulation which is to be prescribed by the Commission, except in the following cases:

(1) where the law so prescribes;
(2) where the consent of the Data Subject has been obtained;
(3) where it is an act that is in compliance with the contract entered into by the Data Subject and the Data Controller;
(4) where it is for the interests of the Data Subject, who is unable to give consent at such time;
(5) where it is a transmission to a person who has been granted a mark certifying the

standards in relation to personal data protection; or

(6) other cases as prescribed by the Commission.

Q10	**Data Localization** Is there any requirement to take custody of P.I. in your country?

No under the present law and the Bill.

Q11	**Security Control** What are the major rules for security control of P.I.

No, under the present law.

According to the Bill, the requirement is that the data controller must establish appropriate secure system to prevent unauthorized access of its PI. There are no requirement to establish privacy policy or appointing a dedicated Privacy Officer.

Vietnam

Tilleke & Gibbins

Waewpen Piemwichai – Foreign Registered Lawyer
waewpen.p@tilleke.com

Q1	**Legal System** (1) Is there a specific law concerning the protection of personal information (P.I.)? (2) What is the effective and/or amended date of such law?

(1) The right to privacy and confidentiality of information is recognized by the Constitution of Vietnam. Currently, there is no single comprehensive law governing the collection, storage and use of personal data in Vietnam. Vietnam's data protection laws are scattered throughout different pieces of legislation. Key legislation include the Civil Code, Penal Code, Law on Network Information Security ("**LNIS**"), Law on Information Technology ("**IT Law**"), Law on Telecommunications, Law on Consumer Protection, Law on E-Transactions, Decree 72 on Internet Services and Online Information, and Decree 52 on E-commerce.

(2) List of relevant legislation

1. Constitution of the Socialist Republic of Vietnam of 2013 adopted by the National Assembly of Vietnam on 28 November 2013 (the "**Constitution**");
2. Civil Code No. 91/2015/QH13 adopted by the National Assembly of Vietnam on 24 November 2015 ("**Civil Code**");
3. Penal Code No. 100/2015/QH13 adopted by the National Assembly of Vietnam on 27 November 2015, effective from 1 January 2018 ("Penal Code");
4. Law on Network Information Security No. 86/2015/QH13 adopted by the National Assembly of Vietnam on 19 November 2015, effective from 1 July 2016;
5. Law on E-Transactions No. 51/2005/QH11 adopted by the National Assembly of Vietnam on 29 November 2005 ("**Law on E-Transactions**");
6. Law on Protection of Consumer Rights No. 59/2010/QH12 adopted by the National Assembly of Vietnam on 17 November 2010 ("**Consumer Protection Law**");
7. Law on Information Technology No. 67/2006/QH11 adopted by the National Assembly of Vietnam on 29 June 2006 ("**IT Law**");
8. Law on Telecommunications No. 41/2009/QH12 adopted by the National Assembly of Vietnam on 23 November 2009 ("**Law on Telecommunications**");

9. Decree No. 52/2013/ND-CP of the Government dated 16 May 2013 on E-Commerce, as amended by Decree No. 08/2018/ND-CP ("**Decree 52**"); and
10. Decree No. 72/2013/ND-CP of the Government dated 15 July 2013 on the management, provision and use of Internet services and online information ("**Decree 72**").

Q2 Definition of "Personal Information"

In the law mentioned in Q1 above, what information is designated as P.I.?

"Personal information" is broadly defined in different pieces of legislation and broadly worded, generally (including advertising and marketing purposes) to be information contributing to identifying a particular individual, including, among other things, name, date of birth, home address, phone number, email address, medical information, ID card numbers, social insurance card numbers, credit or debit card numbers, information on personal payment transactions, and other information that the individual wishes to keep confidential. The phrase "other information that the individual wishes to keep confidential" is problematic in that it seems to give complete subjective discretion to the owners of the information to determine what is considered "personal information".

In addition, in particular for e-commerce activities, "personal information" does not include work contact information and other information that the individual himself/herself has published in the mass media.

Q3 Special Categories of Personal Information (Sensitive Information, etc.)

Is there any special category of P.I. such as sensitive information?

In general, no. Please refer to the definition of P.I. above.

However, in certain sensitive sectors, such as banking, the law categorizes data into general data and sensitive data. Sensitive data is defined as "data containing classified matter, containing information restricted to internal circulation within the entity, or containing information which the entity manages and which, if leaked, could have an adverse impact on the reputation, finances or activities of such entity." The processes and measures handling sensitive data is stricter than general data, such as an entity must take measures to encode information assets containing sensitive data in order to ensure the safety and confidentiality of such information assets during the process of exchange and storing.

Q4	**Consent for Acquisition or Usage** (1) Is consent from the data subject required to acquire P.I.? (2) Is consent from the data subject required to use P.I.?

Yes. Generally viewed, data privacy rules of Vietnam are primitive and repeated among the legislation. The common and key principle across the Vietnamese privacy laws is that the collection, storage, use, processing or publication/disclosure of information and materials related to the private life or personal information of an individual must be consented to by that person , and the use of such information in a network environment (such as a computer network and the Internet) must be in line with the purposes as notified and consented to.

Q5	**Consent for Provision** Is consent from the data subject required to provide P.I. to a third party?

Yes. Transfer of P.I. to a third party must be consented to by the information owner or at the request of a competent authority, or the law provides that it must be transferred.

Q6	**Exceptions for Consent** What are the major exceptions to Q4 and Q5 above?

There are certain circumstances where the collection of personal information can happen without prior consent[2] ("**Consent Exemptions**"):

- collection of personal information already published on e-commerce websites;
- collection of personal information for signing, modifying or performing goods and services purchase and sales contracts with the customers;
- collection of personal information for calculating prices or charges for use of information, products and services which are provided online; and
- performing other obligations in accordance with law.

[2] IT Law, Article 21.3; Decree 52, Article 70.4.

Q7 Information to be Provided

Is there any requirement to provide information upon acquiring P.I.?

If the data will be collected, processed, used, stored or transferred electronically, the IT Law, which is the law governing the use of information technology in a network environment (including providing, transmitting, collecting, processing and exchanging information via information infrastructure, such as telecom networks, the Internet, computer networks, and databases) requires that the person collecting, processing or using personal information of another person must notify such person of the form, scope, place and purpose of the collection, processing or use of his/her personal information (IT Law, Art. 21.2(a)). In addition, as the information can be retained only for a certain period as agreed to by the data subject, the notice should also contain the proposed retention period. If the information will likely be supplied, transferred or disclosed to third parties or any service providers, the notice should contain such transfer or disclosure information as well.

There is no statutory form or template for this notification. In addition, the Law on Network Information Security further provides that if the information is collected, edited, used, stored, supplied, shared or dispersed in the network for "commercial purposes", the organization or individual handling the personal information must develop and publicize their own policies applicable to handling and protection of personal information.

These notifications and privacy policies are not required to be notified to or approved by the regulator, government, or a public entity.

Q8 Transfer to Third Countries

Is there any restriction to transfer P.I. to a foreign country?

Yes, prior consent must be obtained. Vietnam law does not specifically distinguish between the transfer of data within or outside of Vietnam. The rules for the transfer of personal information both within and outside Vietnam are the same. That is, organizations and individuals must 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 data owners, or unless it is at the request of the proper state agencies.

In addition, it is worth noting that the draft Law on Cybersecurity ("**Draft Cybersecurity Law**"), which is under review by the National Assembly at the moment, introduces the principle of data localization to Vietnam. In particular, the Draft Cybersecurity Law provides that foreign

enterprises (companies incorporated outside of Vietnam) when providing telecom and Internet services in Vietnam are required to locate servers on which Vietnamese users' data is administered, within the territory of Vietnam. In addition, in respect of information systems critical to national security (defined vaguely as information systems which, when broken down or sabotaged, will affect national sovereignty, interests and security and seriously impact social order and safety), the owners of such information systems must store personal information and critical data they collected or created within Vietnam. If there is an obligation to provide any information outside of Vietnam, the information system owner must assess security levels as regulated by the Ministry of Public Security ("MOPS") or in accordance with other applicable legislation. However, as a general matter with Vietnamese lawmaking, it is rather uncertain whether legislative drafts will end up becoming law, and, if so, to what extent they will differ. This law is being debated during the current session of the National Assembly. The National Assembly is scheduled to vote on this Draft Cybersecurity Law in the middle of 2018.

Q9 Exceptions for Transfer to Third Counties

What are the major exceptions to Q8 above?

There are certain circumstances where the collection of personal information may proceed without prior consent[3] ("**Consent Exemptions**"):

- collection of personal information already published on e-commerce websites;
- collection of personal information for signing, modifying or performing goods and services purchase and sales contracts with the customers;
- collection of personal information for calculating prices or charges for use of information, products and services which are provided online; and

performing other obligations in accordance with law.

Q10 Data Localization

Is there any requirement to take custody of P.I. in your country?

No.

[3] IT Law, Article 21.3; Decree 52, Article 70.4.

Q11

Security Control

What are the major rules for security control of P.I.

The law generally requires that the person processing personal information in a network environment (such as a computer network and the Internet) must implement managerial or technical measures to ensure that the personal information will not be disclosed, modified, destroyed, lost or stolen. However, there is no further legal guidance on such managerial and technical measures. The party collecting, processing and using personal information can freely assess and implement its own measures.