Deloitte.

Unity in Diversity

The Asia Pacific Privacy Guide

July 2019

Contents

Introduction **iii**

Emerging trends across the region **vi**

Privacy guides by territories **4**

- Australia 6
- Brunei Darussalam 10
- Cambodia 12
- China 13
- Hong Kong 17
- India 22
- Indonesia 24
- Japan 28
- Lao People's Democratic Republic 31
- Malaysia 33
- Mongolia 36
- Myanmar 37
- New Zealand 39
- Papua New Guinea 42
- The Philippines 44
- Singapore 49
- South Korea 52
- Sri Lanka 56
- Taiwan 58
- Thailand 62
- Vietnam 65

Comparison matrix **68**

Regulatory landscape table **69**

Table of primary privacy regulation and regulator **70**

Contacts **73**

Introduction

Introduction

The Asia Pacific region is home to some of the world's fastest growing economies and businesses that are a critical link in the global information economy and supply chain. Organisations in the Asia Pacific also increasingly move information across borders as they look to leverage the different skill sets and capabilities across the region and serve customers globally in the borderless digital economy. More than ever, organisations need to keep informed of the changing and diverse privacy regulatory landscape to minimise their privacy risk, maintain and build trust with customers and build sustainable and productive business networks.

Working locally, thinking globally

While business and technology are increasingly without borders, privacy laws certainly are not. Like the cultures they emanate from, privacy laws differ considerably across the Asia Pacific. This tension between global business needs and local legal requirements gave rise to the OECD's privacy principles back in 1980, but 39 years later there is still considerable work to do before we can begin to imagine a future where privacy laws are 'harmonised'. In developing or strengthening privacy legislation, many countries in the Asia Pacific region have taken inspiration from the European Union (EU) General Data Protection Regulation (GDPR), by either adopting, or planning to adopt, similar or more stringent regulations. An example can be found in Japan, whereby in 2019 it received an adequacy approval from the European Commission, enabling frictionless data sharing between the EU and Japan. In many respects, the GDPR has been the most successful privacy law to date in terms of moving towards global harmonisation and having an impact right across the Asia Pacific region, directly and indirectly.

Introducing this Guide

This Deloitte Asia Pacific Privacy Guide, in its second edition, expands on the original and highlights more granular privacy considerations when handling personal information. The intended audience for this guide are business, risk and compliance specialists who may have privacy management within their remit, but who may not have a deep understanding of the nuances in privacy requirements across the Asia Pacific.

We hope it will be a solid starting point to help guide you in your role but we always encourage consultation with a privacy specialist. Given this is a point in time snapshot of the privacy framework in the region, and to ensure you have the most up-to-date information on requirements, please follow the links to the official resources we have provided for each location, where available.

All information presented within this guide is accurate and up to date as at June 2019.

Emerging trends across the region

The Asia Pacific region is key to the world's business, technological and innovation value chain, with many global corporations leveraging the suppliers and workforce from its varied nations. Jurisdictions such as mainland China, Taiwan, Japan and South Korea are pioneering technologies and processes that leverage personal information for their continued economic success. Singapore, Hong Kong, Tokyo and Sydney are global banking and business hubs. India, the Philippines and Malaysia are leaders in global business support. Understanding that the region must continue to compete in the global market, and at the digital frontier, has led to a rapid development in privacy law and governance. As such, a number of trends have emerged.

Trend 1: Governments are strengthening their privacy law frameworks

The varying levels of personal information protection requirements across the region have raised challenges for organisations, in particular when sharing information across borders. The rapid growth of globalisation coupled with the exponential creation and use of data to fuel business has left some jurisdictions in the region with a privacy governance debt that they are racing to settle.

For example:

- India and Indonesia are currently reviewing their privacy frameworks to consolidate several laws and regulations into single, comprehensive privacy laws.
- Thailand has recently passed a new data protection and privacy legislation that is a significant improvement on the current law.
- New Zealand and Malaysia are currently reviewing their privacy laws to update provisions to align with the technological developments, expectations of individuals and global standards.

How can you prepare?

- Implement a process to identify and assess the impact new regulations or guidelines may have on your business in the jurisdictions that you operate in.
- Consider commissioning a privacy health check to understand how your organisation's privacy framework aligns with the expectations of regulators.
- Implement a data monitoring program and maintain an inventory of personal data that maps data flows within the organisation and to/from third parties throughout the information lifecycle.

Trend 2: Asia Pacific countries are seeking an 'adequacy decision' from the EU

Since the GDPR came into effect, many businesses have had to re-examine their privacy postures. More stringent rules for cross border data transfers mean businesses have had to uplift their privacy capabilities. An 'Adequacy' decision from the European Commission enables the free flow of data between the EU and countries considered 'adequate'. Many are currently seeking to strengthen their laws to obtain an adequacy decision, including South Korea, the Philippines and Taiwan. This will mean less restrictions on the cross-border transfer of personal data for businesses operating within those locations. Currently, New Zealand and Japan are the only countries within the Asia Pacific region with an adequacy decision.

How can you prepare?

- Assess your third party management program in relation to data protection and breach management.
- Assess whether your third parties are compliant with your third party agreements and relevant laws.
- Ensure the required levels of protection and controls are implemented when transferring data cross-border.

Trend 3: Alignment across the region

The Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) system was developed to build customer, business and regulator trust in the cross border flow of personal data. Businesses participating in the CBPR system are required to create privacy policies and frameworks consistent with the APEC Privacy Framework. Once certified by accountability agents, it will create a similar impact as having adequacy under the EU GDPR by enabling cross-border data flows.

Adopting the CBPR system will mean organisations will be able to demonstrate to their customers that a minimum level of protection of personal information has been adopted. This may be a key differentiator with competitors.

How can you prepare?

- Consider whether your organisation has privacy protections in place that are aligned with the standards promoted by self-regulatory initiatives such as the APEC Cross-Border Privacy Rules.
- Consider consolidating your organisation's data management practices when operating across multiple jurisdictions so that they align with best practice regionally and/or globally.

Trend 4: Mandatory data breach notification laws

As business in the region becomes increasingly digitalised and processes are moved online, cyber-attacks and data breaches are becoming as great a risk here as they are anywhere else in the world. The rise of data breaches globally, in frequency and volume, has put pressure on governments to introduce mandatory data breach notification requirements. In early 2018, Australia enacted a mandatory data breach notification scheme. Malaysia, Singapore, New Zealand and Thailand are currently looking to introduce a mandatory notification scheme for data breaches.

How can you prepare?

- Consider creating a data breach response plan using the guidance provided by the regulators who have jurisdiction over your business.
- In order to ensure your plan meets the most stringent data breach laws and all relevant provisions are considered, review your data breach response plan.
- Understand your risk culture and ensure staff within your organisation are aware of their role in responding to a data breach.

Trend 5: Greater recognition for the rights of individuals

There has been an improvement in the recognition of the right to privacy in the digital age with respect to how individuals can access or control their data. The rise in data breaches and privacy-related incidents has facilitated discussion around how much control people really have over their personal information and consequently raised awareness among the general public. There has been a push for more comprehensive rights for individuals, such as the right to request suspension of processing and the right to erasure.

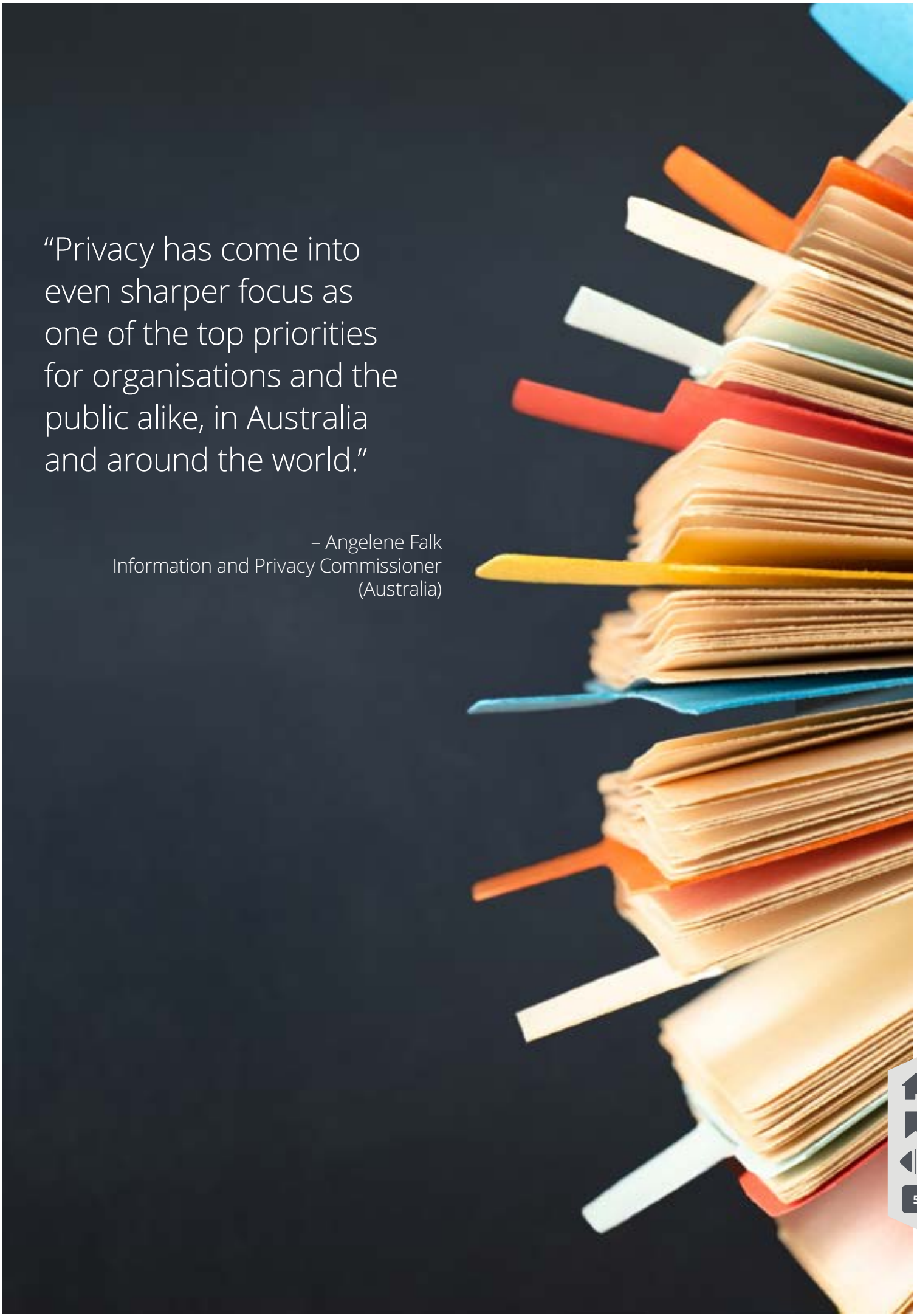
India and Thailand have drafted bills that introduce comprehensive rights that significantly augment the current rights available to individuals. Most prominently, the right to data portability has become almost necessary for many countries that wish to participate in a data-driven economy with initiatives such as open banking. Australia, India and Singapore have started to look into introducing such an initiative to meet the demands of consumers in the market.

How can you prepare?

- Consider being more transparent with your customers regarding how you use their data.
- Implement a process for customers to communicate to your organisation in the event that they would like to exercise a right in relation to their personal information, such as to access or correct their personal information.

Privacy guides by territories

Australia
Brunei Darussalam
Cambodia
China
Hong Kong
India
Indonesia
Japan
Lao PDR
Malaysia
Mongolia
Myanmar
New Zealand
Papua New Guinea
The Philippines
Singapore
South Korea
Sri Lanka
Taiwan
Thailand
Vietnam



"Privacy has come into even sharper focus as one of the top priorities for organisations and the public alike, in Australia and around the world."

– Angelene Falk
Information and Privacy Commissioner
(Australia)

Australia

Privacy in Australia is primarily regulated through a comprehensive federal law, centred on principles known as the Australian Privacy Principles ('APPs'). The Commonwealth Privacy Act 1988 (Cth) ('Privacy Act') applies to private sector entities with an annual turnover of at least AU $3 million and all Federal Government agencies. Most states and territories in Australia (excluding Western Australia and South Australia) have their own privacy laws, which are applicable to state government agencies.

Personal information is also protected under other legislation including the Workplace Surveillance Acts and Health Records Acts, which are governed at the State level.

Primary legislation: Privacy Act 1988 (Cth)

Considerations

- **Privacy Act reforms:** Australia introduced mandatory data breach reporting in February 2018. Since then, there has been a 712% increase in the number of reported data breaches and 964 eligible data breaches from 1 April 2018 to 31 March 2019.[1]
- **Open banking:** Open banking will officially begin in Australia from 2020 introducing a consumer data right (CDR), helping individuals to easily compare products and services by giving them greater control over their information to extract it. This will be a gradual roll out, impacting the larger banks first. Banks will be expected to make credit card, debit card, deposit and transaction account data available under the open banking regime. As a result, consumer financial institutions are rethinking their approach to privacy.
- **Federal Government Agencies Privacy Code (the Code):** The Code, effective from July 2018, sets out specific requirements for Federal Government agencies to implement privacy governance. For example, the Code requires agencies to have a privacy management plan, appoint a privacy officer and privacy champions, and undertake a privacy impact assessment (PIA) for all high risk projects.
- **Online privacy:** There are no laws or regulations in Australia specifically relating to online privacy. If cookies or other similar technologies, collect personal information, the organisation is required to comply with the Privacy Act for collection, use, disclosure and storage. The Privacy Commissioner provides detailed guidelines on this.[2]

Definition of personal information

The Privacy Act defines 'personal information' as information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion:

- is true or not; and
- is recorded in a material form or not.

Sensitive information is recognised as a specific type of personal information, which includes information or an opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, health information and tax file number information.

Collection and notice

Personal information, other than sensitive information, should only be collected if it is reasonably necessary for a specified purpose. Sensitive information must not be collected unless certain conditions are met. This may occur where consent has been collected from the individual or if collection is required by law. If an organisation receives unsolicited personal information, it is required to determine whether the information should be retained, de-identified or destroyed.

At or before the time of collection, or as soon as practicable, an organisation is required to provide notification to individuals. Notification must include details of the organisation, the purpose for which personal information is collected, who the personal information will be shared with, what rights individuals will have over that information (i.e. access, correction etc.) and how they can exercise their rights.

[1] The Office of the Australian Information Commissioner, Notifiable Data Breach Scheme 12-Month Insights Report.

[2] https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

Use and disclosure

Personal information can only be used for the original purpose it was collected for, unless certain conditions are met – for example, if an individual consents to a secondary use of their personal information or if further use is required by law. If the organisation uses or discloses personal information for a secondary purpose, the individual should be provided with a written notice of use or disclosure.

Direct marketing

If personal information is used for direct marketing, organisations are required to ensure:

- Communications include a simple means and at no cost to opt out.
- Requests to opt out are honoured.

Data retention and destruction

Personal information must be kept up to date, complete and accurate. The information should not be kept longer than is necessary to fulfil the purpose it was collected for. If no longer required for a particular purpose, the information should be securely destroyed or de-identified.

Individual rights

Individuals have the right to:

- **Be informed** of their rights prior to collection and use of their personal information through notification.
- **Access and correct** their personal information, and organisations must respond within 30 days or inform individuals that they are unable to do so within the timeframe.

Security

Organisations must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. The Privacy Commissioner provides guidance on what is considered reasonable in the context of securing personal information.[4]

Data breach notification

On the 22nd of February 2018, the mandatory data breach notification regime commenced in Australia. The Commissioner and data subjects must be notified for breaches concerning personal information, credit reporting information, credit eligibility information and tax file numbers.

Requirements	
Threshold for reporting	• Organisations must notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of data breaches likely to result in serious harm to an individual. • Serious harm is not defined in legislation. However, the OAIC provides guidance for interpreting and assessing serious harm.[3]
Time frame	• If an organisation suspects a data breach meets the threshold, an assessment must be conducted within 30 days. • Organisations must notify the OAIC and affected individuals as soon as practicable.
Who to notify	• When there are reasonable grounds to believe a data breach that meets the threshold has occurred, the Commissioner and affected individuals must be notified.
Content	• Notification must include the contact details of the organisation, a description of the breach, types of information concerned and steps to be undertaken by individuals.

Cross-border data transfer

Personal information can only be transferred to another organisation outside of Australia where reasonable steps have been taken by the transferring organisation to ensure the overseas recipient does not breach the Privacy Act.

Governance

Organisations are not required to appoint a data protection officer (DPO). However, the Commissioner has recommended that organisations appoint a DPO as good practice. Organisations must manage personal information in an open and transparent way. Reasonable steps must be taken to implement practices, procedures and systems to ensure organisations comply. This may involve dealing with inquiries from individuals and maintaining a clear, up-to-date and accessible privacy policy.

Regulators and regulatory landscape

The OAIC is the Australian regulator of privacy led by the Australian Information Commissioner. The Commissioner's roles and responsibilities involve:

- Conducting investigations into acts, which may breach the Privacy Act.
- Managing complaints about the handling of personal information.
- Providing privacy advice to the public, government agencies and businesses.

[3] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

[4] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information

Cases

- **2017 –** A telecommunications company refused to provide a former journalist with metadata following a right of access request. As a result, the Commissioner, on behalf of the journalist, argued for a broad interpretation of personal information in court. Specifically, it was argued that any information which is able to identify an individual should be protected under the Privacy Act. The Federal Court ruled in favour of the telecommunications company and the Administrative Appeals Tribunal because the request to access pertained to information about the service provided by the company as opposed to the journalist himself.
- **2018 –** In April, the acting Commissioner launched a formal investigation into a social media company following confirmation that the information of over 300,000 Australian users may have been acquired and used without authorisation.

Penalties

- The Commissioner will investigate an act or practice that may interfere with the privacy of an individual and a complaint about the act or practice has been made.
- The Commissioner may also investigate any breaches of the Privacy Act on its own initiative (where an individual has not made a complaint).
- Where the Commissioner undertakes an investigation of a complaint which is not settled, it is required to ensure that the results of that investigation are publicly available. This is undertaken by publishing the investigation report on the OAIC website.
- After investigating a complaint, the Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organisation rectify its conduct or that any loss or damage suffered by the individual is compensated.
- Fines of up to AU $420,000 for an individual and AU $2.1 million for corporations may be requested by the Commissioner and imposed by the Courts for serious or repeated privacy breaches.

Terminology

Terminology	Definition
Agency	'Agency' refers to Australian government (and Norfolk Island government) agencies, but does not include State and Territory agencies.
APP entity	An 'APP entity' is defined to be an agency or organisation required to comply with the Australian Privacy Act 1988.
Organisation	An 'organisation' is defined as: • An individual (including a sole trader) • A body corporate • A partnership • Any other unincorporated association, or • A trust unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Freedom of Information Act 1982	Government	Office of the Australian Information Commissioner (OAIC)	Government
My Health Records Act 2012	Health sector	Office of the Australian Information Commissioner (OAIC)	Health care providers
Privacy Credit (Reporting Code) 2014	Financial services	Office of the Australian Information Commissioner (OAIC)	Credit providers (CP) and Credit reporting bodies (CRBs)
Prudential Practice Guide CPG 235 Managing Data Risk	Financial Services	Australian Prudential Regulation Authority (APRA)	Financial Services
Prudential Standard CPS 234 Information Security	Financial Services	Australian Prudential Regulation Authority (APRA)	Financial Services
SPAM Act 2003 (Cth)	All	Australian Communications and Media Authority	Comprehensive
Telecommunications Act 1977	Telecommunications	Office of the Australian Information Commissioner (OAIC)	Telecommunications carriers and carriage service providers
Telecommunications (Interception and Access) Act 1979	Telecommunications	Office of the Australian Information Commissioner (OAIC)	Telecommunications carriers and carriage service providers
Workplace Surveillance Act (NSW) 2005	All	NSW Industrial Relations Commission	Employers
Workplace Privacy Act (ACT) 2011	All	WorkSafe ACT	Employers
Surveillance Devices (Workplace Privacy) Act 2006 (VIC)	All	Victoria Police	Employers
Health Records and Information Privacy Act (NSW) 2002	All	Information and Privacy Commission (NSW)	Public and private sectors handling health information
Health Records Act (VIC) 2001	All	Health Complaints Commissioner (VIC)	Public and private sectors handling health information
Health Records – Privacy and Access Act (ACT) 1997	All	ACT Human Rights Commission	Public and private sectors handling health information
Privacy and Personal Information Protection Act 1998 (NSW)	Government	Information and Privacy Commission (NSW)	State based public sector agencies
Information Privacy Act 2014 (ACT)	Government	Office of the Australian Information Commissioner (OAIC)	State based public sector agencies
Privacy and Data Protection Act 2014 (VIC)	Government	Office of the Victorian Information Commissioner	State based public sector agencies
Information Privacy Act 2009 (QLD)	Government	Office of the Information Commissioner (QLD)	State based public sector agencies
Information Privacy Principles (SA)	Government	State Records of South Australia	State based public sector agencies
Information Act (NT)	Government	Office of the Information Commissioner (NT)	State based public sector agencies
Information and Protection Act 2004 (TAS)	Government	Tasmanian Ombudsman	State based public sector agencies

Brunei Darussalam

The protection of personal information is currently guided by the Data Protection Policy 2014 (DPP), which applies to agencies. However, a Minister at the Prime Minister's Office acknowledged that an improved legal framework to protect personal data is required, especially given the implications arising from well-known global data breaches related to social media platforms.[5]

In January 2019, the Minister of Transport and Info-communications confirmed that he was appointed as the Minister responsible for cyber security of the nation, encompassing safeguarding of personal data. Brunei's awareness and direction moving towards privacy and personal data protection regulations has primarily risen as a response to cities holding more personal data of its citizens.

Further, the Brunei government has considered privacy and data protection frameworks from neighbouring countries, including Malaysia and Singapore, to incorporate in their own design of laws and regulations for the future. However, the progression of this anticipated legislative reform is yet to be formerly announced.

Primary legislation: Data Protection Policy 2014

Considerations

Online verification portal development: In March 2018, the Prime Minister's Office revealed a plan to establish an online portal to limit the spread of fake news on social media, amidst data misuse cases globally and within neighbouring Asia Pacific countries.

Definition of personal data

The DPP defines personal data as data, whether true or not, about an individual who can be identified:

- from the data; or
- from the data combined with other information which the agency holds or is likely to come into possession of.

Collection and notice

Personal data should be collected where necessary by fair and lawful means. This includes the requirement to obtain consent from the individual. Collection should be limited to fulfil specific purposes.

At or before the time of collection or as soon as practicable, agencies should communicate to individuals the purpose for collection and how the data will be used and disclosed. However, if the purpose for collection has not been provided initially, agencies should provide this to the relevant individual prior to use.

Data retention and destruction

Personal data should be retained only if it is necessary to fulfil the purpose for which it was collected. However, agencies can develop internal policies, guidelines and procedures for the retention and destruction of data. Upon destroying data, reasonable care should be exercised by agencies to prevent unauthorised access.

Use and disclosure

The individual must be informed and have provided consent to the agency prior to any use or disclosure taking place. However, where it is impracticable to obtain the individual's consent, a legal guardian or power of attorney can provide consent on their behalf. This also applies where personal data will be used and/or disclosed to a third party, except where:

- The collection, use or disclosure is clearly in the interest of the individual and it is impracticable to obtain the individual's consent.
- Legal, medical or security reasons make it impossible or practical to obtain consent.
- An emergency that threatens life, health or security of an individual exists.
- The data is generally publicly available.
- Use or disclosure is necessary to render a service applied for by the individual.
- Disclosure is made to an institution, whose purpose is for the conservation of records of historic or archival importance, and disclosure is for such purpose.

Individual rights

Individuals have the right to:

- **Be informed** of their rights prior to collection and the intended use of their personal data.
- **Access** their personal data.

Security

Agencies should ensure all data is protected, regardless of its held format, to prevent accidental or unlawful loss, unauthorised access, disclosure, use or modification. In doing so, it is important for employees to also be made aware of the significance to maintaining data confidentiality. Methods of protection may be physical, organisational and/or technological.

[5] https://thescoop.co/2018/05/10/brunei-calls-legal-framework-protect-user-data-online/

Data breach notification

Although the DPP does not specify requirements for data breach notification, it does state that non-compliance with the DPP should be reported to the administrator by designated agency officers.

Cross-border data transfer

Agencies are only permitted to transfer personal data to a party outside of Brunei if:

- There is a reasonable belief that the recipient is subject to a law, binding scheme or contract, which upholds principles for fair data handling substantially similar to the DPP;
- The individual has provided consent;
- It is necessary for contract performance or pre-contractual obligations; and
- Reasonable steps have been taken to ensure the data will not be used, held or disclosed by the recipient inconsistent to the DPP.

Governance

Agencies must designate an officer to ensure the agency complies with its privacy policy.

Regulators and regulatory landscape

Currently, there is no regulator for privacy. However, the DPP guidance is regulated by the Minister at the Prime Minister's Office ('Authority') and the Minister of Transport and Info-communications who have recently been appointed for upholding responsibilities and expectations related to cyber security within Brunei.

Roles and responsibilities of the authority and administrator involve:

- Administering and enforcing the DPP in addition to providing regular reports.
- Promoting government awareness.
- Performing non-compliance or breach related investigations and providing recommendations to remedy or prevent such occurrences.
- Providing consultancy, advisory, technical, managerial and/or other special services.
- Advising the government on the above matters and representing the government internationally.
- Conducting research and promoting educational activity.

Relevant laws, regulations and standards

Law/ regulation or standard	Industry	Regulator	Applicability
APEC Privacy Framework 2015	All	APEC	Personal information controllers, individuals, organisations and member economies
ASEAN Framework on Personal Data Protection 2016	All	ASEAN	Participants
Computer Misuse Act 2007 (revised)	All	Minister of Finance	Persons
Electronic Transactions Act 2008 (revised)	All	Minister of Finance/ Controller	Persons
Tabung Amanah Pekerja Act 1999	Employment/ Retirement	The board of directors of theLembaga Tabung Pekerja (LTAP)	Employees and employers

Terminology

Terminology	Definition
Administrator	Refers to the E-Government National Centre.
Agency	Any government ministry or department including educational institutions and statutory body.
Controller	The Controller of Certification Authorities appointed under section 41(1) and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section 41(2) of the Electronic Transactions Act 2008.
Data	Information in electronic or manual form.
Employee	Any person, a citizen or permanent resident of Brunei Darussalam, employed under a contract of service or apprenticeship or other agreement to work for an employer.
Employer	The person whom an employee entered into a contract of service or apprenticeship with.
Individual	A natural person to whom the data relates to, living or deceased.
Participants	ASEAN member states including the Telecommunications and IT Ministers of Brunei Darussalam, the Kingdom of Cambodia, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Republic of the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand and the Socialist Republic of Vietnam.
Personal information controller	A person or organisation who controls or instructs another person or organisation to collect, hold, process, use, transfer or disclose personal information.

Cambodia

Cambodia does not currently have legislation specifically providing for the protection of personal information. Information privacy is currently only covered by sector-specific laws, which contain provisions protecting customer and confidential information but not specifically personal information. A law is currently being drafted to provide individuals with the right to access their personal information.

Considerations

- **Sector-specific regulation:** While there is no national privacy legislation, there are sector-specific regulations that regulate customer data. For example, in the banking and financial sector, there are laws to prohibit the disclosure of confidential information and specific requirements for correction and security of consumer data.
- **New e-commerce legislation:** An e-commerce law is currently in draft to regulate online electronic transactions and contains provisions that address consumer data and data protection.
- **Proposed access to information law:** Cambodia is proposing to introduce a freedom of information law to enable individuals to request access to information held by public bodies.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Law on Telecommunications 2015	Telecommunications	Ministry of Post and Telecommunications	Telecommunications organisations and individuals
Law on Cyber Security (24/2018/QH14)	Banking and Finance	National Bank of Cambodia	Banking and financial institutions
Law on Information Technology (67/2006/QH11)	Banking and Finance	National Bank of Cambodia	Credit reporting institutions handling consumer data

China

When operating in China, organisations should be aware of the complexity of the regulatory landscape. China has a complex web of regulations and rules and this varies depending on the location. There are also other requirements in sector-specific laws which address the protection of personal information.

The protection of personal information is regulated by the People's Republic of China Cybersecurity Law 2017 ('CSL'). The CSL has broad application and applies to network operators – most businesses that operate with a computer network e.g. intranet – and critical information operators.

China's rapid adoption of technologies, such as artificial intelligence and biometric technology, has given rise to a privacy specific law. However, the timeframe for this law is yet to be publicly announced. The focus of this anticipated law will be directed heavily towards protecting biometric data, given the prevalence of surveillance cameras and facial recognition technology within the country.

Primary legislation: People's Republic of China Cybersecurity Law 2017

Considerations

- **Law across sectors, provinces and nationally:** Organisations are required to adhere to and stay up to date with the obligations prescribed under law and regulations. Guidelines are also published to support the laws, and organisations are also required to adhere to these. Staying informed of developments in regulations and guidelines is imperative to operating in China.
- **Increasing awareness of privacy rights:** The Chinese public are increasingly aware of their privacy rights, particularly following high profile court cases. For example, a consumer rights group recently took legal action against a technology company for infringing upon the rights of its users by collecting excessive personal information without consent.[6]
- **Applications:** The National Principal Security Committee, China Consumers Association, China Internet Association and China Cyberspace Security Association were commissioned to form the "APP Governance Working Party" on the 25th of January 2019 and subsequently released the "Guideline to Self-assessment of App Collection and Use of Personal Information" on the 1st of March 2019.

Definition of personal information

Personal information is defined as any information which can be used to identify a person, either separately or combined with other information. This can include information contained within electronic records. Examples of personal information are: a natural person's name, date of birth, personal identification information, address and telephone number.

Collection and notice

Network operators must collect personal information:

- In a legal and proper manner.
- Where necessary i.e. information must not be collected unless it relates to the network operator's services.
- In accordance with agreements created between users.
- Upon approval/ consent by the person to which the information applies to.

Upon collecting personal information, network operators are required to provide users with a notification, which specifies:

- The purpose of collection.
- How information will be collected.
- How information will be used.

[6] https://www.scmp.com/tech/china-tech/article/2127045/baidu-sued-china-consumer-watchdog-snooping-users-its-smartphone

Use and disclosure

Personal information must only be used for the original purpose for which it was collected or for a directly related purpose. Network operators can use information outside of this scope for a new purpose, so long as voluntary and explicit consent has been provided by the user.

Direct marketing

The CSL does not explicitly refer to direct marketing. However, it is recognised that network operators must not illegally provide information to others without the approval of the person whose personal information is collected. This requirement does not apply where the information is de-identified and cannot be recovered.

Data retention and destruction

Personal information must be accurate, kept up to date and should not be kept longer than necessary to fulfil the purpose for which it was collected.

Individual rights

Individuals have the right to:

- **Be informed** of their rights prior to collection and use of their personal information.
- **Request correction and removal** of their personal information.

Security

Network operators must take practicable steps to protect personal information from unauthorised or accidental access, processing, erasure, loss or use. Such steps may include implementing controls, such as encryption and multi-factor authentication.

Data breach notification

Data breach notification to the regulator and affected individuals is mandatory.

Requirements	
Threshold for reporting	Where there is a reasonably foreseeable real risk of harm or damage from a breach. This is determined by: • The amount and kinds of information leaked • Circumstances of the breach itself • The likelihood of identity theft or fraud • Whether the information is adequately encrypted, anonymised or otherwise rendered inaccessible • Whether the breach is ongoing and if there will be further exposure of personal information • Whether the breach is an isolated incident or a systematic problem • Whether information has been retrieved before being accessed or copied • Whether effective mitigation or remediation was conducted after the breach • The ability of users to avoid or mitigate possible harm • A reasonable expectation of users' privacy
Time frame	• Network operators should provide notification as soon as practicable, except where law enforcement agencies have requested delay for investigative purposes.
Who to notify	Depending on the circumstances, network operators should notify: • Affected users • Law enforcement agencies • Relevant regulators • Any other parties who can take remedial action to mitigate impact of the breach
Content	Depending on circumstances, notification should include: • A general description, including the time and duration of the breach and its discovery • The source of the breach and types of personal information involved • An assessment of the risk of harm presented • A description of measures taken to prevent further harm • The network operator's contact information • Information and advice about further steps which users should take • Whether law enforcement agencies and other relevant parties have been notified

Cross-border data transfer

Network operators can only transfer personal information once users have been informed and have authorised for the transfer to occur. However, any information collected and generated within China must stay within its borders. If information is required to be transferred outside of China, a security assessment must be conducted in accordance with measures formulated by the Cyberspace Administration of China (CAC).

Governance

The appointment of a DPO is not required. However, a network operator or CIIO must be appointed.

Regulators and regulatory landscape

The CAC is the regulator of privacy within China led by the Director. The Director's roles and responsibilities involve:

- Creating cyberspace policy.
- Acting as the central internet regulator.
- Providing regulatory oversight and censorship.

Cases

- **2018 –** An online forum, microblogging site and social media messaging app were summoned by the CAC for failing to block various types of illegal internet information, described as vulgar and harmful.
- **2019 –** The CAC ordered telecommunication operators to shut down services for up to 8,000 mobile applications which were said to have stolen users' personal information.

Penalties

Orders to correct, warnings and fines may be issued under the CSL, depending on what article has been breached. However, any serious breach may result in fines of up to ¥1,000,000.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Decision on Strengthening Online Information Protection	All	CAC	Network Operators and CIIOs
GB/T 35273—2017 Information Technology – Personal Information Security Specification	All	CAC	All organisations
National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services	All	CAC	Network Operators and CIIOs

Terminology

Terminology	Definition
Critical information infrastructure operators (CIIO)	Any industry-related operators, such as public communications and information services, energy, transport, water conservancy, finance, public services, e-government, and other important industries, where breaching their information infrastructure would result in serious damage to national security, national economy and people's livelihood and public interests.
Network	Any system composed of computers or other information terminals and related equipment, which execute procedures of information collection, storage, transmission, exchange and processing.
Network operator	Any owners or managers of the network and network service providers.

"Organisations should uphold the attitude of the three Data Stewardship Values for handling personal data. Such approach would not only reinforce consumer trust but also exemplify organisations' commitment to personal data privacy protection and realise the principle of accountability, thereby elevating their reputation and increasing their competitiveness."

– Stephen Kai-yi Wong
Privacy Commissioner for Personal Data (Hong Kong)

Hong Kong

Hong Kong has one of the most comprehensive privacy regimes in Asia, with a principles-based law supported and enforced by the Office of the Privacy Commissioner of Personal Data (PCPD). The primary privacy legislation was enacted in 1996 in response to the European Union Data Protection Directive and underwent major reform in 2012 to incorporate additional provisions. In response to multiple data breaches and the changing global privacy regulatory landscape, the regulator is currently reviewing the PDPO.

Primary legislation: Personal Data (Privacy) Ordinance (PDPO)

Considerations

- **International legislation:** Taking inspiration from international regulations, the Commissioner has demonstrated an intention to review international privacy laws and bring the PDPO into alignment. In particular, the EU GDPR and China's cyber security laws are on the radar of the Commissioner.
- **Review of the PDPO:** The Commissioner is looking to review the PDPO following major data leaks and cyber-attacks in Hong Kong. One consideration is increasing penalties for non-compliance (the current maximum is HK$50,000).
- **Industry regulators:** Industries have increased their focus on cyber security and privacy. Industry regulators like the Security and Futures Commission (SFC) have included data protection clauses in their framework to ensure proper data handling practices.
- **A turn towards data ethics:** Following high profile breaches in 2018, the Commissioner has declared that '[d]ata ethics can … bridge the gap between legal requirements and the stakeholders' expectations.' The Commissioner has recently published a research report supporting an Ethical Accountability Framework.

Definition of personal data

Personal data is defined as information that:

- relates to a living person (known as a data subject);
- can be used to, directly or indirectly, identify them; and
- is in a form in which accessing or processing the data is practicable.

The PDPO does not define 'sensitive' data. However, there are codes of practice issued to regulate data such as Hong Kong Identification Card numbers and unique identifiers, including passport numbers and patient numbers.

The Commissioner has issued specific guidance on biometric data, stating that data can only be collected when necessary, and with free and informed consent to collect it from the data subject.

Collection and notice

The collection of data must be:

- In a lawful and fair manner.
- Directly related to an activity of the data user.
- Necessary, but not excessive, for the related purpose.

Organisations are required to provide information to the individual about whether it is mandatory to give the data and the consequences of not providing it. Data subjects must be notified of the purpose of collection and use, and the classes of persons to whom the data may be transferred.

Use and disclosure

Personal data can only be used for the original or a directly related purpose, unless voluntary and explicit consent is provided by the data subject for the new purpose.

If personal data is used or disclosed for a new purpose (i.e. a purpose other than the purpose for which the data was to be used at the time of the collection or a directly related purpose), prescribed consent must be obtained from the data subject. Prescribed consent means express consent given voluntarily which has not been withdrawn in writing.

Direct marketing

If personal data is used for direct marketing, explicit consent needs to be collected from the data subject, however, silence does not constitute consent.

Bundled consent, where the data subject must provide personal data in order to access the product or service, is not a valid form of consent.

The data subject is required to be informed of:

- The intention to use their information for direct marketing.
- Types of data that will be used.
- What the marketing will be about.
- Method for the data subject to communicate consent for the intended use.
- Withdrawal of consent is allowed at any time.

If personal data is being sent to a third party for direct marketing, the data subject's consent needs to be in writing.

Data retention and destruction

Personal data is required to be kept up to date and accurate, and should not be kept longer than necessary to fulfil the purpose for which it is collected.

The Privacy Commissioner's Office has provided guidance on retention of CV's for unsuccessful job applicants. The Equal Opportunities Commission's Codes of Practices on Employment recommend retention of employment application records for at least one year. The Privacy Commissioner considers this retention period to be reasonable for the purpose of responding to any claim of discrimination.[7]

Individual rights

Data subjects have the right to:

- **Be informed** of their rights at, or prior to, collection and use of their data, the retention period, the security measures in protecting their data and how they can raise an access and correction request.
- **Access and correct personal data:** organisations must respond to requests within 40 days or inform the individuals that they are unable to do so within the timeframe.

Security

Organisations must take practicable steps to protect personal data from unauthorised or accidental access, processing, erasure, loss or use. The following factors should be considered:

- Kind of data and the harm when data is inadequately protected
- Security measures incorporated into data storage equipment
- Secure transmission of data
- Physical location of the data storage
- Measures for assurance of integrity, prudence and competence of people who could access data

[7] https://www.pcpd.org.hk/english/resources_centre/publications/guidance/fact2_hrm_2.html

Data breach notification

There is currently no requirement to notify data subjects or the PCPD of a data breach. However, the PCPD could conduct an investigation relating to a breach and issue an enforcement notice if appropriate. The Commissioner has recommended voluntary notification in the event of a data breach.

Voluntary guidance	
Threshold for reporting	Reasonably foreseeable real risk of harm or damage from breach, depending on: • Kind of personal data leaked • Amount of personal data involved • Circumstances of data breach • Likelihood of identity theft or fraud • Whether leaked data is adequately encrypted, anonymised or otherwise rendered inaccessible • Whether data breach is ongoing and if there will be further exposure of data • Whether the breach is an isolated incident or systematic problem • In the case of physical loss, whether personal data has been retrieved before accessed or copied • Whether effective mitigation or remediation was conducted after breach • Ability of data subjects to avoid or mitigate possible harm • Reasonable expectation of personal privacy of data subjects
Time frame	As soon as practicable • Except where law enforcement agencies have requested delay for investigative purposes
Who to notify	(Depending on circumstances) • Affected data subjects • Law enforcement agencies • Commissioner • Relevant regulators • Other parties who can take remedial actions to mitigate the impact of the breach
Content	(Depending on circumstances) • General description • Data, time and duration of breach • Date and time breach discovered • Source of breach • Types of personal data involved • Assessment of risk of harm from breach • Description of measures taken to prevent continued breach • Organisation's contact information for more information/assistance • Information and advice on further steps data subjects should take • Whether law enforcement agencies, PCPD and other parties have been notified

Cross-border data transfer

Organisations can only transfer personal data if data subjects are informed when personal data is collected that:

- Their personal data may be transferred; and
- The classes of people to whom it may be transferred to.

The PDPO prohibits cross border transfer of data except in specified circumstances. However, that provision has not yet been enacted. The PCPD currently provides a 'Guidance on Personal Data Protection in Cross-border Data Transfer'[8] to outline best practices for the cross-border transfer of data. For example, the PCPD recommends organisations review data transfer agreements and to keep an inventory of personal data.

Governance

There is no mandatory requirement to appoint a data protection officer.

However, the PCPD advocates for companies to be accountable for the protection of personal data to build trust with clients, enhance reputation and increase competitiveness.

Regulators and regulatory landscape

The Office of the Privacy Commissioner for Personal Data (PCPD) is the independent statutory privacy regulator tasked with enforcement of the PDPO. The PCPD's roles and responsibilities include:

- Enforcement
- Monitoring and supervising compliance
- Promotion of education, training and best practice
- Corporate governance
- Meeting changing needs relating to technological developments, trends and expectations

[8] https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf'

Cases

- **2017 –** The Kowloon City Magistrates' Court found that a company director was held personally liable and convicted for failing to comply with a lawful requirement (in this case, a summons) of the Privacy Commissioner and fined HK$3,000.
- **2018 –** The Tuen Mun Magistrates' Court fined a supermarket chain HK $3,000 for using personal data in direct marketing without obtaining consent.
- **2018 –** In November, the Commissioner found reasonable grounds to believe there was a 'contravention of a requirement under the law' by an airline and commenced a compliance investigation (ongoing).

Penalties

A serious breach of the PDPO may result in financial penalties of up to HK $1m and imprisonment of up to five years if an individual is found personally liable for the violation.

Relevant law, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Personal Data Privacy Ordinance	All	PCPD	Data users
Code of Practice on the Identity Card Number and other Personal Identifiers: Compliance Guide for Data Users	All	PCPD	Data users
Control measures for customer data protection	Banking and Finance	HKMA	Authorised institutions under the Banking Ordinance
Code of Practice on Consumer Credit Data	Banking and Finance	PCPD	Credit providers and credit referencing agency
Code of Practice on Human Resource Management	All	PCPD	Employers
Guidance on Personal Data Protection in Cross-border data Transfer	All	PCPD	Data users
Guidance on Collection and Use of Biometric Data	All	PCPD	Data users
SFC Compliance with the Personal Data (Privacy) Ordinance	Banking and Finance	SFC	Licensed corporations under SFC

Terminology

Terminology	Definition
Codes of Practice	Practical guidance in respect of requirements under this Personal Data (Privacy) Ordinance.
Data users	A person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data. The data user is liable as the principal for the wrongful act of its authorised data processor.
Ordinance	Legislative enactments.

"The digital economy should aim to benefit citizens. With proliferation of information and digital technologies, the technology sector should strengthen citizen safety and security in the digital environment. Moreover, user awareness towards their privacy has been on the rise. We will see consumers making more privacy-conscious decisions and associating certain brands that provide greater privacy controls as better options."

– Rama Vedashree
CEO of Data Security Council of India

India

A specific privacy law does not exist in India. However, the Information Technology Act 2000 presently governs the protection of personal information, specifically electronic data and transactions. The prominence of data use has placed privacy and data protection high on the national agenda and is key to India's growth and economic development. For example, the government has expressed an inclination towards creating a digital health technology ecosystem by releasing the draft Digital Information Security in Healthcare Act (DISHA), the primary focus of which is to regulate the process of collection, storing, transmission and use of the digital health data.

As a result, a new data protection law, known as the Data Protection Bill 2018, has been drafted. The Data Protection Bill 2018, in combination with the Draft National E-Commerce Policy, proposes to strengthen the protection of personal information and consumer rights, as well as impose conditions on cross-border data transfers by requiring data fiduciaries to store data in India. They will help to regulate the use of personal data collected, disclosed, shared or processed in India or in connection to business within India. The Bill introduces stringent requirements related to mandatory data breach notification, consent to be obtained prior to collection and individual privacy rights.

Primary legislation: Information Technology Act 2000

Considerations

Constitutional right to privacy: The Supreme Court delivered a judgment in relation to constitutional rights. It was interpreted that the right to privacy is an extension of the right to life provided by the Constitution. This includes the right of an individual to exercise control over his or her personal data. As a result, there is an obligation to ensure the protection of a citizen's right to privacy.

Definition of personal information

Personal information is defined as information relating to a natural person, directly or indirectly, in combination with other available information or likely to be available with a body corporate, capable of identifying a person.

Sensitive information is defined as information provided to a corporation related to an individual's password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, or biometric information.

Collection and notice

Organisations must obtain written consent from individuals prior to collection. They must also take reasonable steps to notify the individual concerned that their information is being collected, the purpose of collection and details of the recipient. Organisations must provide a privacy policy to the individual and publish it on their website. Sensitive information must not be collected by organisations unless necessary for a lawful purpose connected with a business function.

Use and disclosure

Organisations must only use sensitive information for the purpose declared when it was collected. Consent must be obtained before disclosing sensitive information unless required under contract or where necessary to comply with a legal obligation. An organisation may be legally required to provide personal or sensitive information to government agencies for purposes such as verifying identification, preventing, detecting and investigating cyber incidents, or administering punishment.

Data retention and destruction

Organisations must not retain sensitive information for longer than necessary.

Individual rights

Individuals have the right to:

- **Access, correct and amend** their personal information.
- **Refuse and withdraw consent** for the use of personal information at any time.

Security

Organisations must demonstrate compliance with reasonable security practices and procedures. This can be achieved by implementing and documenting comprehensive information security programs and policies containing adequate controls for the business' information assets. For example, the international standard ISO 27001 is recognised as a standard that organisations must comply with.

Data breach notification

Data breach notification is not required under the Act. However, an incident may be voluntarily reported to the Computer Emergency Response Team (CERT) by service providers, intermediaries, data centres, body corporate and any other person. CERT is a national agency, which has been granted power under the Act to respond to cybersecurity incidents. Notification content may include:

- Time of the incident
- Symptoms observed
- Information regarding the affected system/s or network/s
- Actions taken to mitigate damage
- Other relevant technical information, such as the security systems used

Cross-border data transfer

Organisations can transfer sensitive information to receivers adhering to the same level of data protection, where required by law, under contract or consent has been obtained.

Regulators and regulatory landscape

There is no dedicated privacy regulator in India. However, adjudicating officers are appointed by the government to determine contraventions with the ITA and its Rules, and can impose penalties.

Cases

- **2016 –** A pathology lab had over 35,000 electronic medical records leaked. As a consequence, the laboratory erased all records and closed 250 of its centres in Mumbai in addition to over 10,000 collection points across India.
- **2018 –** An Indian government database holding personal information (including biometrics and demographic data, such as fingerprints and iris scans amongst names, addresses etc.) for over 1 billion citizens and its authority suffered a data breach. The World Economic Forum Global Risks Report 2019 labelled this breach as 'the largest data breach' ever. Privacy concerns arose in relation to the corresponding mobile application concerning significant flaws within the app. A student was arrested for accessing this database without authorisation in August 2017.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Electronic Health Record Standards For India 2016	Health	Ministry of Health and Family Welfare (MHFW)	Individuals
The Clinical Establishments (Registration and Regulation) Act 2010	Health	MHFW	State governments, persons, the Authority, clinical establishments
The Draft National E-Commerce Policy, 2019	Electronic commerce	Department for Promotion of Industry and Internal Trade	The Indian Government as a whole and entities within
The Information Technology (Reasonable security practices and procedures and Sensitive Personal Data or Information) Rules 2011	All	The Central Government of India	Body corporates and persons in India

Terminology

Terminology	Definition
Clinical establishment	Includes a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called that offer services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognised system of medicine established and administered or maintained by any person or body of persons, whether incorporated or not.
Cyber incident	Any adverse event related to cybersecurity that violates a security policy. Such event may involve unauthorised access or DDoS amongst other forms.

Indonesia

Privacy and data protection is currently governed by provisions across a set of regulations. The regulations include:

- The Government Regulation No. 82 of 2012 ('Gov. Reg. 82')
- Electronic Information and Transactions Law No. 11 of 2008 ('EIT Law')
- MOCI Regulation No. 20 of 2016 (Protection of Personal Data in an Electronic System) ('MOCI Regulation')

These regulations only apply to personal data on electronic systems.

A comprehensive law is currently in draft and will consolidate privacy and data protection requirements into a single legislation.

Considerations

- **A constitutional right to privacy** is contained within Indonesia's Constitution.
- **A proposed comprehensive data protection framework currently in draft:** A comprehensive law on data protection (Bill on the Protection of Private Personal Data/ PDP Draft Law) is being prepared jointly by the Ministry of Law and Human Rights and the Ministry of Communication and Informatics (MOCI). If passed, the law will become the first comprehensive law in Indonesia to deal explicitly with data privacy.
- **National regulating authority:** While there are various authorities presently operating with privacy related functions, there is no privacy regulator. MOCI is presently considered the main regulatory body. MOCI operates with the function of overseeing data protection activities within Indonesia. The draft data protection law introduces a Commission with functions to ensure protection of personal data.

Definition of personal data

Personal data is defined as data of an individual which is stored, maintained and kept accurate.

In addition, a further definition is provided for 'certain data of an individual', which is any information that is correct, actual and can directly or indirectly identify an individual.

Collection and notice

Personal data should only be collected if it is relevant and suitable for the purpose for which it was collected.

Consent is required for the collection, use, processing and transfer of personal data. Consent must be express and in writing, and to be provided manually or electronically. In order to obtain consent, an electronic system provider provides a consent form prior to collection. Parents or legal guardians can provide consent in cases where the individual is not capable of providing consent, such as minors or disabled persons.

Notice must be provided to individuals at the time the personal data is collected. The notice should include:

- Details about the current and possible future purposes for collection of personal data; and
- The organisation's contact details.

Use and disclosure

Personal data can only be used and processed in accordance with the purpose provided in the notice when personal data was collected.

Further, personal data can only be used after its accuracy and suitability has been verified.

The electronic system operator (ESO) must obtain consent from an individual for data to be handled or disclosed to a third party.

Data retention and destruction

An ESO that provides services to public bodies must establish a data centre and disaster recovery centre in Indonesia.

Personal data is to be deleted upon expiry of the storage period provided at time of collection, unless it is still required for the intended purpose, or when the data owner has made a request to do so.

Individual rights

Individuals have the right to:

- **Submit complaints** to the Minister of Communication and Informatics (MOCI) regarding the failure of an ESO to protect personal data.
- **Access and update** their personal data without interference.
- **Request a historic view of the data collected** by the ESO.
- **Request destruction** of their personal data handled by the ESO.

Exceptions apply to the above rights, which mainly refer to situations where other laws and regulations request an ESO to perform differently.

Security

An exhaustive list of ESO obligations for maintaining security is contained within both Gov. Reg.82 and the MOCI Reg. 20. Broadly, regulations impose an obligation for organisations to:

- Obtain certification of its electronic systems to ensure compliance.
- Maintain the correctness, validity, confidentiality, accuracy, relevance and compatibility with the purpose personal data was collected for.

Cross-border data transfer

The transfer of data outside of Indonesia must comply with reporting and coordination requirements. The following must be reported:

- The name of the country to which information will be transferred to
- Details of the recipient
- Details about the transfer itself including the intended date and purposes of the transfer

Consent must also be obtained for transfer.

Parties may enter into data transfer agreements, however there is no mandatory clause or approved content that needs to be incorporated into the agreements.

The transfer of personal data managed by an ESO at a government institution must be coordinated with the MOCI or the authorising institution and comply with prevailing laws and regulations regarding cross-border exchange of personal data.

Data breach notification

There is a mandatory data breach notification requirement for operators of electronic systems. The regulatory authority of the sector in which the ESO operates and the affected data owners must be notified if there is a potential to cause loss.

Requirements	
Threshold for reporting	• The operator must notify individuals if the breach has potential to cause loss to the individual. • The operator must notify if any failure, serious system interference or disturbance equates to the breach of personal data.
Time frame	• The operator must notify the affected individuals no later than 14 days after the breach was identified. • The operator must notify the relevant authority of the sector in which they operate in immediately.
Who to notify	• Electronic system operators must notify: – Data subjects. – Supervising and regulatory authority of the relevant sector, or law enforcement.
Content	• The operator is to provide, in writing, to affected individuals: – The cause of the personal data breach.

Governance

There is no requirement for the appointment of a DPO.

Regulators and regulatory landscape

There is currently no national data protection authority for privacy in Indonesia. The MOCI governs the regulations covering data protection relating to electronic systems. MOCI carries the ability to investigate matters, which involve the unlawful handling of personal and confidential information, and have power to impose administrative sanctions such as fines.

Cases

2018 – An investigation was launched into the alleged data breach where a company is believed to have obtained the personal data of one million Indonesian users from a social media platform. The scandal is believed to have affected up to 87 million users worldwide. A class action lawsuit was commenced against the social media company in an Indonesian District Court.

Penalties

Breaches of the MOCI Reg or Reg 82 will attract administrative sanctions, such as verbal or written warnings, temporary suspension of processing activities and public announcements. The EIT Law imposes criminal penalties for certain violations, such as unlawful access.

Key laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Financial Service Authority Regulation No. 1/ POJK.07/2013	Financial services	Financial Services Authority	Financial service providers
Government Regulation No. 82 of 2012 (Provisions of Electronic System and Transactions)	All	MOCI	Electronic system operators
Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law)	All	MOCI	Electronic system operators
Law No. 19 of 2016 on Amendment of EIT Law	All	MOCI	Electronic system operators
Law on Health No. 36/2009	Health	Ministry of Health	Health providers
Law on Telecommunications No. 36/1999	Telecommunications	MOCI	Telecommunication service providers
MOCI Regulation No. 20 of 2016 (Protection of Personal Data on Electronic Systems)	All	MOCI	Electronic system operators

Terminology

Terminology	Definition
Electronic system operator (ESO)	Any private person, state operator, enterprise, or element of society who makes available, manages, and/or operates an electronic system either privately or communally for the electronic system's users for his/her own benefit, or a third party's benefit.

"Businesses are required to more strictly manage personal information, as their increasingly globalised operations result in more frequent transmission of such data between (Japan and) overseas."

– Harumichi Yuasa
Professor at the Institute of Information Security Yokohama

Japan

In Japan, privacy is regulated by the Act on the Protection of Personal Information ('APPI'). The APPI is a comprehensive privacy law, administered by the Personal Information Protection Commission ('PPC'), and applies to personal information handling business operators ('PIHBO') to protect the interests of principals.

The PPC has issued an interim draft report, which revealed plans for Japan to revise its existing personal information protection law in 2020. The focus will be to introduce a right to be forgotten, which would be applied cross Japan's borders.

Primary legislation: Act on the Protection of Personal Information 2017

Considerations

EU adequacy: On the 23rd of January 2019, the European Commission confirmed its adequacy decision for Japan, which finds that the scope of data protection in Japan and the EU are equivalent. This decision will create, develop and facilitate opportunities for European and Japanese businesses to share data. The decision was supported by supplementary Rules that strengthened the APPI. The supplementary rules included additional protection for new types of sensitive personal information.

Definition of personal data

Personal information is defined as information, which relates to a living individual, and can fall within any of the following:

- Where containing a name, date of birth or other description, in vocal or written format, through drawing or electromagnetic record, to include scenarios where the information can be collated with other information to identify a specific individual
- Where containing an individual identification code

The APPI also defines special care-required personal information ('sensitive information'), which includes personal information comprising of an individual's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions.

Collection and notice

The APPI refers to the collection of personal information as proper acquisition. PIHBOs must not obtain personal information by deceit or improper means. PIHBOs must promptly and explicitly inform the principal whose personal information was acquired of the utilisation purpose, including where the purpose has changed. However, this notice requirement does not apply in cases where there exists an urgent need to protect human life, body or fortune, or where the utilisation purpose was previously disclosed to the public.

PIHBOs must obtain the principal's consent before collecting sensitive information. Consent is not required where:

- Information is required by laws and regulations.
- There is a need to protect human life, body or fortune and it is difficult to obtain the principal's consent.
- There is a special need to enhance public hygiene or promote the fostering of healthy children and it is difficult to obtain the principal's consent.
- Government and/or enforcement related cooperation is required and obtainment of the principal's consent would interfere with such performance.
- The information is publically available.
- Prescribed by cabinet order.

Use and disclosure

Personal information must be used for a specific purpose stipulated at the time of collection. However, personal information can be used for a new purpose if consent is obtained from the principal or where any of the above exceptions (provided in collection and notice) apply.

Data retention and destruction

Personal information must be kept accurate and up to date to the extent that it is necessary to achieve its purpose.

PIHBOs are required to delete personal information, without delay, once the utilisation purpose has been fulfilled.

Specific industry codes and standards also specify requirements for the retention and destruction of personal information.

Individual rights

Individuals have the right to:

- **Be informed** of their rights prior to collection and use of their personal information.
- **Request correction, rectification and/or deletion** of their personal information held by PIHBOs.
- **Object to processing** by lodging a utilisation cease request, based on reasonable grounds.
- **Lodge complaints** to the PPC or any other authorised entity about the handling of their personal information.

Security

PIHBOs must take necessary and appropriate actions to protect personal information from leakage, loss or damage. For example, PIHBOs must exercise necessary and appropriate supervision over employees who handle personal information, to prevent unauthorised access or misuse.

Cross-border data transfer

Personal information must not be transferred to a third party unless consent has been obtained from the principal or any one of the above exceptions apply, as provided within 'Collection and notice'.

Personal information may be transferred outside of Japan where:

- Consent is obtained from the principal.
- The foreign state has privacy laws which are considered equivalent to Japan.
- The foreign party maintains an internal personal information protection system consistent with standards set by the PPC.

Data breach notification

While there is no mandatory breach reporting scheme, the PPC provides voluntary guidance (Guidelines for the Act on Protection of Personal Information) for PIHBOs to undertake assessment, remediation and reporting of breaches as best practice.

Voluntary guidance	
Threshold for reporting	Where there is a reasonably foreseeable real risk of harm or damage from breach, depending on: • Kind and amount of personal information leaked • Circumstances of data breach • Likelihood of identity theft or fraud • Whether leaked information is adequately encrypted, anonymised or otherwise rendered inaccessible • Whether the data breach is ongoing and if there will be further exposure • Whether the breach is an isolated incident or a systematic problem • In the case of physical loss, whether personal information has been retrieved before accessed or copied • Whether effective mitigation or remediation was conducted after the breach • Ability of principals to avoid or mitigate possible harm • The reasonable expectation of a principal's personal privacy
Time frame	• As soon as practicable, except where law enforcement agencies have requested a delay for investigative purposes
Who to notify	• Affected data subjects • Commissioner • Relevant regulators or law enforcement agencies • Other parties who can take remedial action to mitigate the impact
Content	• Information involved, time, date, duration and discovery of the breach • Source of breach • Assessment of risk of harm from the breach • Description of measures taken to prevent continued breach • Organisation's contact information for more information/assistance • Information and advice on further steps principals should take • Whether law enforcement agencies and other parties have been notified

Regulators and regulatory landscape

The regulator is the Personal Information Protection Commission (PPC).

The Commissioner's roles and responsibilities include:

- Formulating and promoting policy
- Supervising
- Mediating complaints
- International cooperation
- Public relations
- Conducting personal information protection assessments
- Issuing accreditations to organisations
- Reporting

Cases

- **2018 –** Several online retailers encountered a data breach when hackers targeted weaknesses on the retailers' websites. Approximately 15,000 customers were affected where credit card information was compromised including individual names, expiration dates and security codes. The Japan Consumer Credit Association estimated total losses from stolen credit card related personal information at ¥18.7 billion in 2018 alone.
- **2019 –** A marketing research company operating in Tokyo suffered a leak of over 570,000 records of personal information, including email addresses, passwords and phone numbers.
- **2019 –** A car manufacturer made a public notification for a data breach caused by third party attackers through its dealerships. The breach was limited to unauthorised access of computer systems, which led to compromised personal information of over 3.1 million customers, including names, birth dates and employment information.

Relevant laws, guidelines and rules

Law, guideline or rule	Industry	Regulator	Applicability
Act on the Protection of Personal Information held by Administrative Organs	Public Sector	PPC	National government bodies
Act on the Protection of Personal Information held by Independent Administrative Agencies	Public Sector	PPC	Independent administrative agencies
Act on Specified Commercial Transactions	Commerce	Japan Consumer Affairs Agency	Organisations
Act on the Regulation of Transmission of Specified Electronic Mail	Commerce	Ministry of Internal Affairs and Communications	Organisations
APPI Supplementary Rules for the Handling of Personal Data Transferred from the EU	All	PPC	Business operators handling personal data of EU data subjects
Enforcement Rules for the Act on the Protection of Personal Information	All	PPC	Personal information handling business operators and principals
Guidelines for the Act on Protection of Personal Information (PPC Notices No. 6-9 of 2016)	All	PPC	Personal information handling business operators and principals

Terminology

Terminology	Definition
Individual identification code	Prescribed by cabinet order to include any character, letter, number, symbol or other codes, which are able to identify a specific individual and can be assigned to the use of services or purchase of goods sold or provided to an individual or stated in a card or other document.
Personal information handling business operator	A person providing a personal information database for use in business but excludes a central government organisation, a local government and an incorporated (local or not) administrative agency.
Principal	A specific individual identifiable through personal information.
Utilisation purpose	The purpose of use for the personal information that is provided to an individual at the time of collection/ acquisition.

Penalties

Penalties for business operators can include:

- Up to one year imprisonment or a maximum fine of ¥500,000 for disclosing personal information for the purpose of illegal profit.
- Up to six months imprisonment or a maximum fine of ¥300,000 for a business operator violating an order from the PPC.
- Up to six months imprisonment or a maximum fine of ¥300,000 for a business operator failing to submit or providing false reports to the PPC upon request.
- Penalties may also apply to representatives of a business operator, such as an individual employee.

Lao People's Democratic Republic

Lao PDR has some basic regulation in place to protect personal information. The Law on Prevention and Combating Cyber Crime (Cybercrime Law) 2015 prohibits the use of personal information which may cause reputational harm to an individual.

Further, the Law on Electronic Data Protection 2017 (EDPL) contains requirements around personal information collection, storage, maintenance, use, dissemination, transfer, access, amendment, update and deletion of electronic data.

Primary legislation: The Law on Electronic Data Protection 2017

Definition of personal information

Personal data refers to the electronic data of an individual, legal entity or organisation.

Collection and notice

Personal data can only be collected by an individual, legal entity or organisation where it is approved by the data owner.

The individual, legal entity or organisation must inform the data owner of the purpose for collection.

Use and disclosure

A data administration authority can use or disclose personal data where the data owner has approved the purpose for which it will be used or disclosed, unless required otherwise by law.

Data retention and destruction

Personal data must be deleted:

- When requested by the data owner.
- When it is no longer required for the purpose it was collected for.

Individual rights

Data owners have the right to:

- Request access or update their personal data.
- Request deletion of personal data.

Security

A data administration authority is required to maintain the security of its systems to protect data. The security measures required include:

- Using technical systems to secure the data
- Inspecting and evaluating risk of data systems on an annual basis
- Investigating incidents that have caused or may cause serious impact

Regulators and regulatory landscape

The Ministry of Posts and Telecommunications (MPT) is responsible for the administration of the EDPL. The Ministry has duties such as developing policy, enforcing the provisions through administrative measures and regularly reporting electronic data protection activities to the government.

Penalties

Individuals, legal entities or organisations found to violate the provisions of the EDPL can be fined up to 15,000,000 Kip. The regulator also has powers to enforce the law through administrative measures, such as disciplinary sanctions, warnings and re-educational measures.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Framework on Personal Data Protection	All	ASEAN	Participants and organisations
Guidelines on the Implementation of the Law on Electronic Data Protection 2018	All	MPT	Data managers
Instruction on Computer Security under the Law on Prevention and Combating of Cyber Crime	All	MPT	Businesses
Law on Prevention and Combating Cyber Crime 2015 (The Cybercrime Law)	All	MPT	Persons, legal entities and organisations
Law on Electronic Transactions 2012	All	Ministry of Science and Technology	Individuals, legal entities, state organisations and agencies, international organisations and civil society
Penal Law 2005	All	Lao PDR government	All individuals within Lao PDR

Terminology

Terminology	Definition
Data owner	Individual, legal entities or organisations that own the electronic data.
Electronic data administration authorities	An individual, legal entity or organisation responsible for administrating the electronic data which mainly are ministries, data centre through internet, telecommunication service providers and banks.

Malaysia

Malaysia is governed by a comprehensive privacy regime, based on the provisions of Personal Data Protection Act 2010 ('PDPA'). The PDPA is principles-based and applies to any person who processes and has control over or authorises the processing of personal data within commercial transactions, namely data users. The Act does not apply to Federal and State government bodies, personal data processed outside of Malaysia (unless intended to be used for processing in Malaysia) and credit reporting agencies.

The Privacy Commissioner has introduced a public consultation paper to introduce a data breach notification scheme.

The review of the PDPA commenced in late 2018 and is expected to reach Parliament by mid-2019 to align with global legislation such as the General Data Protection Regulation (GDPR).

Primary legislation: Personal Data Protection Act 2010 ('PDPA')

Considerations

Data user registration: There is a requirement for data users to be registered before processing personal data. Registration certifications are valid for one year after which registration must be renewed. Data users who require registration fall within key industries, including communications, banking and financial institutions, insurance, health, tourism and hospitalities, transportation, education, direct selling, services, real estate and utilities.

Definition of personal information

Personal data includes any information that:

- Relates, directly or indirectly, to a data subject.
- The data subject can be identified or identifiable from, alone or combined with other information held under possession of the data user.

Sensitive data is personal data, which consists of:

- Information about the physical or mental health or condition of a data subject.
- Political opinions.
- Religious or other similar beliefs.

Collection and notice

Personal data can only be collected where necessary or for a lawful purpose, which is directly related to and not excessive of, one or more of the data user's activities.

A data user must provide notice to the data subject as soon as practical to notify them of the following:

- Types of data collected
- The purpose for collection
- Information about the data as a source
- Data subject rights to access, request correction and lodge complaints
- Whether the data will be disclosed to third parties and whom
- Ways to limit the use and processing of the data
- Whether supplying the data is voluntary or not and what consequences will arise if data is not provided

Use and disclosure

Data users should take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up to date. Personal data cannot be processed by data users unless the data subject has provided consent to such processing.

Processing of personal data occurs for:

- Contract performance, which the data subject is a party to or intends to enter into.
- Compliance with any other legal obligation.
- Protecting the interest of the data subject.
- The administration of justice.

Data users must not process sensitive data unless it is necessary to protect the data subject's vital interests and where consent cannot be obtained.

Personal data cannot be disclosed without the consent of the data subject for any purpose other than or directly related to the purpose specified at the time of collection.

Data retention and destruction

Data users have the responsibility to take reasonable steps to ensure personal data is either destroyed or permanently deleted if and once it is no longer required for the purpose for which it was collected for.

Individual rights

Data subjects have the right to:

- **Be informed** of their rights prior to collection and use of their personal data through notification.
- **Access and correct** personal data held by the data user.
- **Withdraw consent** to data processing. For example, data subjects may prevent processing where it is likely to cause damage or distress, or where processing is for direct marketing purposes.

Security

Data users are required to take steps to ensure personal data is protected from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. For example, the Personal Data Protection Standard 2015 states that all employees must be registered if they process personal data. Further, data users should provide sufficient guarantees to data subjects regarding the technical and organisational security measures, which will govern data processing. In doing so, steps must also be taken to ensure compliance with the above and data users should consider the following:

- Harm likely to arise from the above implications
- Where the data is stored
- Security and other measures to ensure reliability, integrity and competence of personnel who have access to the data
- Measures to ensure secure transfer of the data

Cross-border data transfer

Personal data cannot be transferred outside of Malaysia unless otherwise provided by the Minister upon recommendation of the Commissioner and by notification published in the Gazette, or where one of the following conditions is met:

- The data subject has provided consent
- Transfer is necessary for contract performance between the data user and subject
- The data user has taken reasonable grounds and exercised due diligence to ensure personal data will not be processed in contravention of the PDPA
- Transfer is necessary to protect the vital interests of the data subject or is within the public interest as determined by the Minister

Regulators and regulatory landscape

The Personal Data Protection Department (PDPD) and the Malaysian Communications and Multimedia Commission (MCMC) jointly hold responsibility as regulators for privacy and data protection in Malaysia:

- MCMC is led by the Minister
- PDPD is led by the Personal Data Protection Commissioner

The Commissioner's roles and responsibilities involve:

- Advising the Minister on national personal data policy.
- Implementing and enforcing the PDPA.
- Monitoring and supervising compliance with the PDPA.
- Investigating complaints.

The Personal Data Protection Advisory Committee also plays a role in the regulatory landscape by advising the Commissioner on matters relating to personal data protection and the enforcement of the Act.

Cases

- **2017 –** In May, a private college was charged by the PDPD for processing personal data of a former employee without a valid certificate of registration, which is a breach under section 16 of the PDPA and is the first case where a data user has been charged under the Act.
- **2017 –** Malaysia's largest data breach, affecting more than 46 million mobile phone subscribers from the country's biggest mobile service provider, occurred from 2014 and was reported in 2017. Personal data was advertised for sale on the dark web and on a technology news website. Additionally, the personal data of 80,000 individuals was leaked from well-known health organisations. Types of data offered for sale included mobile, home and work numbers, identification card numbers, residential and work addresses and SIM card data.
- **2018 –** Personal data of over 1 million university students and alumni from a local university was breached through a leak online. Types of data involved in this breach include names, student IDs, addresses, mobile phone numbers, campus codes and names, program codes and course level details.

Penalties

Violations of the PDPA are punishable with criminal liability and can include fines and/or imprisonment, depending on the section of the Act breached. Where the processing of personal data does not comply with the Personal Data Protection Principles in the PDPA, punishment may be imposed in the nature of a fine not exceeding RM 300,000 or in the nature of imprisonment for a term not exceeding 2 years, or both.

Relevant laws, regulations and standards

Standard	Industry	Regulator	Applicability
Personal Data Protection Standard 2015	All	Commissioner	Data users

Terminology

Terminology	Definition
Data user	Any person who processes and has control over or authorises the processing of personal data within commercial transactions.

Mongolia

The law pertaining to privacy and data protection in Mongolia is limited. The Personal Secrecy (Privacy) Act 1995 contains limited protections for the privacy of individuals but only as it relates to certain categories of information, which gives it a narrow scope. It provides protections of 'personal secrets', which are categorised into information such as correspondence, health, property, family and other secrets prescribed by law. Disclosure of that information is generally prohibited except for national security purposes and to protect public health or legitimate interests.

Considerations

- **Open data:** In 2013, Mongolia implemented an open government partnership initiative by joining the Open Government Partnership to increase transparency and reduce corruption. This was followed by an open data initiative in 2014 which included open data projects across multiple government agencies.
- **Organisational privacy:** The Organisation Secrets Act 1995 allows organisations to designate data, including personal data not covered in the main privacy legislation, as 'organisational secrets' which require protection. This law restricts their use and disclosure with associated offences for breach, indirectly creating an obligation for information security.

Cases

2018 – A group of hackers infiltrated a Mongolian government data centre which was used to compromise government resources, including government websites.

Relevant laws, regulations and standards

Law, regulation and standard	Industry	Regulator	Applicability
Criminal Code of Mongolia	All	N/A	Everyone
Information Transparency and the Freedom of Information Act	All	N/A	Everyone
Law of Mongolia on Telecommunications	All	N/A	Everyone
Organisations' Secrets Act 1995	All	N/A	Organisations
Personal Secrecy (Privacy) Act 1995	All	N/A	Everyone

Myanmar

While Myanmar does not have specific privacy laws, the Law Protecting the Privacy and Security of the Citizen, enacted in March 2017, prohibits the interception of a citizen's electronic communications, private correspondences and physical privacy, unless otherwise warranted by an order. This law applies to public bodies such as the Ministry of Home Affairs (MOHA) and government departments. The law is not comprehensive due to a lack of provisions to govern how personal information should be managed throughout the information lifecycle.

Considerations

- **Government power:** Prohibitions under the Law Protecting the Privacy and Security of Citizens can be bypassed with permission from the President or a government body. Also, the Telecommunications Law empowers the Ministry of Communications and Information Technology (MCIT) to control and access information transmitted by telecommunication services and their equipment.
- **Defamation and social media:** The Telecommunications Law and the Law Protecting the Privacy and Security of the Citizens have been used, primarily by government officials, to argue defamation where social media users for example have posted criticising comments in relation to the State or its officials.

Use and disclosure

Unless otherwise provided, no person shall:

- Have their communication with another person or related equipment intercepted or disturbed.
- Request or obtain personal telecommunications or any other electronic data from telecommunication operators.
- Open, search, seize or destroy another person's private correspondences, such as an envelope, package or parcel.

Citizens specifically should not be held under surveillance, spied on nor investigated to the extent that their privacy, security and/or dignity would be disturbed.

Regulators and regulatory landscape

The MOHA and the Ministry of Communications and Information Technology (MCIT) are the shared regulators of privacy within Myanmar and must undertake roles and responsibilities together to:

- Protect the privacy and security of citizens from damage unless provided for by existing law.
- Receive and handle complaints in accordance with this law.

Cases

2015 – An employee from a telecommunications company was terminated after sharing a customer's call log outside of the company. The company pursued legal action against the ex-employee for breaching her employment contract and its code of conduct.

Relevant laws, regulations and standards

Law, regulation and standard	Industry	Regulator	Applicability
Telecommunications Law	Telecommunications	MICT	All people, departments and organisations within the Union, and all Myanmar citizens outside of the country

Terminology

Terminology	Definition
Agency	Any Government Ministry or Department including educational institutions and statutory body.
Data	Information in electronic or manual form.
Personal Information Controller	A person or organisation who controls or instructs another person or organisation to collect, hold, process, use, transfer or disclose personal information.

"Privacy and data protection is about the ability to exercise autonomy and control over your personal information. Clearing the slate, and removing data collected at an earlier time, under different terms and conditions, for different purposes, is an expression of that autonomy and control."

– John Edwards
Privacy Commissioner (New Zealand)

New Zealand

In New Zealand, privacy is primarily regulated by the Privacy Act 1993 ('Privacy Act'), which contains principles on how agencies should collect, use, disclose, store, retain and provide access to personal information. This framework is comprehensive and principles-based.

The Privacy Commissioner is currently reviewing this Act as a result of growing concerns for protection of personal information in the digital environment. The Bill is currently in its second reading. The Privacy Act will better align to certain requirements contained within the GDPR, notably mandatory data breach notification. New offences, increased penalties and greater enforcement power for the Commissioner will also be incorporated into the law as part of this Bill.

Primary legislation: Privacy Act 1993

Considerations

- **Tort law:** Courts have developed a tort where a person can sue another for a breach of privacy. This was notably demonstrated in the case of Hosking v Runting (2004). The tort contains two elements, which must be proven. First, there must exist a reasonable expectation of privacy in accordance with the facts of the case. Second, there must be an occurrence of publicity, which is considered highly offensive to an objective reasonable person. The burden of proof rests upon the victim's ability to prove the breach caused real harm, distress or humiliation.
- **Adequacy status:** In 2012, the European Commission formally declared that New Zealand law provides an adequate standard of data protection for the purposes of European Union (EU) law. This means that personal data can be transferred from any of the 27 EU member states to New Zealand for processing without further safeguards required. However, the EU will be re-evaluating New Zealand's adequacy status upon amendments made to the Privacy Act.
- **Unique identifiers:** Unique identifiers, such as customer, driver's licence and passport numbers, must not be assigned to individuals unless necessary for the agency to carry out any of its functions efficiently. Also, agencies are prohibited from requesting a unique identifier from an individual unless disclosure is required for a purpose related or directly related to the assignment of the identifier.
- **Guidelines for landlords and tenants:** The Office of the Privacy Commissioner (OPC) has produced guidelines for landlords inspired by guidance from the Canadian Office of the Privacy Commissioner, which outlines what information should and should not be collected when deciding whether an individual will be a suitable tenant or not. For example, the collection of bank statements to determine an individual's ability to pay rent is permissible. However, collecting bank statements to determine money management style is unfair and unreasonably intrusive.

Definition of personal information

Personal information includes any information about an identifiable individual, such as a name, date of birth, address, biometric information and/or gender etc. If there is a reasonable chance someone could be identified from the information, it is personal information. This also applies to individuals whose death is maintained pursuant to the Birth, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

Collection and notice

Personal information can only be collected where necessary for a lawful purpose and directly from the individual.

At the time of collection, or as soon as possible, agencies must take reasonable steps to notify individuals of the following:

- The occurrence of collection
- Purpose of collection
- Intended recipients
- Contact details of the collector and holder of information
- Any law requiring collection, and if so, whether it is voluntary or mandatory
- Possible consequences if all or part of the information is not provided
- Their rights to access and correct information collected and held about them

Use and disclosure

An agency must not use or disclose personal information without taking reasonable steps to validate that it is accurate, complete, relevant, up to date, and not misleading. The agency must not use the information for a purpose other than the one it was collected for.

Personal information must not be disclosed unless:

- Associated with, or directly related to, the original purpose of collection
- Information was obtained from a publicly available publication
- It is directed to and approved by the individual concerned
- Approved by the Privacy Commissioner

Data retention and destruction

Personal information must be destroyed once its purpose for collection has been fulfilled.

Security

An agency is required to ensure personal information is protected against loss, misuse, disclosure, unauthorised use or unauthorised disclosure through reasonable security safeguards while considering physical, electronic, operational, transmission and destruction-related security.

Individual rights

Individuals have the right to:

- **Be informed** of their rights prior to collection and the intended use of their personal information.
- **Access and correct** personal information held about them.

An agency may refuse to disclose personal information for a range of reasons. For example, if the disclosure is not authorised by the individual concerned or where the disclosure would lead to a serious threat to public health or safety.

If an agency refuses to correct personal information, the individual can request a statement to be attached to the original information saying why correction was refused.

Data breach notification

Data breach notification is not mandatory. However, the Office of the Privacy Commissioner (OPC) provides guidance about responding to a data breach as best practice. This is summarised in the table below.

Voluntary guidance	
Threshold for reporting	• Reporting should occur where personal information has been inappropriately accessed, collected, used or disclosed. The following factors should be considered: – Legal and contractual obligations to the individual – Risk of harm to the individual – Whether there is a reasonable risk of identity theft or fraud, physical harm, significant humiliation or loss of dignity, damage to the individual's reputation or relationships – Whether the individual has the ability to avoid or mitigate possible harm
Time frame	• Agencies should provide notification as soon as possible so that individuals can take steps to protect themselves and regain control of their information
Who to notify	• The OPC should also be notified in the event of a data breach. • Notification should also be made directly to affected individuals by phone, letter, email or in person. • Alternatively, if direct notification can cause further harm, indirect notification should be made through websites, notices or media
Content	Notification should include: • Details about the incident and types of compromised personal information • Actions taken by the agency to control or reduce harm • Steps to inform, guide and protect individuals • Contact information for enquiries, complaints and the OPC • Appropriate support when necessary e.g. advice on changing passwords

Cross-border data transfer

Once transferred, personal information should not be held, used or disclosed unless it falls within or is directly related to the scope of the original purpose for collection. Security controls must be in place to ensure personal information is safeguarded from misuse or disclosure to another party.

The OPC has the power in exceptional cases to restrict cross-border transfer of personal information from New Zealand by issuing a transfer prohibition notice if:

- It believes the receiving party does not provide protections contained within or comparable to the Privacy Act
- The transfer would likely contravene the basic principles set out by the OECD with regard to using and security personal information

Governance

Agencies are required to appoint a privacy officer. The privacy officer is responsible for:

- Encouraging compliance with the Privacy Act
- Dealing with requests made to the agency, such as access and correction
- Working with the Commissioner in relation to investigations

Penalties

The Privacy Commissioner prefers to settle a complaint by conciliation and mediation in the first instance. If a complaint cannot be settled in this way, a formal investigation may be conducted to form an opinion. The Privacy Commissioner does not have the power to issue a formal ruling or determination and cannot begin prosecution proceedings or impose a fine. The proposed Privacy Amendment Bill will increase the penalty for non-compliance with investigations from the Office of the Privacy Commissioner from NZ $2,000 to $10,000.

The opinion outlined by the Privacy Commissioner is not legally binding but is highly persuasive. If the opinion is that there has been an inference with privacy, the Privacy Commissioner may refer the matter to the Director of Human Rights who may then decide to take the complaint to the Human Rights Review Tribunal (HRRT). The Tribunal will hear the complaint and its decision is legally binding. It can award damages to a maximum of NZ $350,000 for breaches of privacy. The most the HRRT has awarded thus far for a privacy matter is NZ $168,000.

Regulators and regulatory landscape

The PCO is the New Zealand regulator of privacy led by the Privacy Commissioner. The Commissioner's roles and responsibilities include:

- Making public statements on privacy matters
- Inquiring and investigating matters, such as complaints, which may affect individual privacy
- Endorsing and promoting privacy understanding
- Monitoring privacy impacts of new technologies and new legislation
- Developing codes of practice within specific industries and sectors
- Monitoring and assessing government data matching programmes

Recent cases

- **2018 –** In March, the Commissioner claimed that a social media website breached provisions of the Privacy Act for failing to respond to an individual's request for information and cooperating with the investigation. The Commissioner deleted his social media account after a decade of use, due to his privacy concerns.
- **2018 –** In December, the Sensible Sentencing Trust (SST) falsely labelled a man as a convicted paedophile on its website. The Commissioner referred the complaint to the Director of Human Rights Proceedings and publicly named the SST in accordance with the PCO's naming policy to warn the public of the SSTs inadequate approach to privacy.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Civil Defence National Emergencies (Information Sharing) Code 2013	Public sector	OPC	Agencies
Credit Reporting Privacy Code	Credit Reporting	OPC	Credit reporters
Health Information Privacy Code 1994	Health	OPC	Health agencies
Justice Sector Unique Identifier Code	Public sector	OPC	Justice sector agencies
Superannuation Schemes Unique Identifier Code	Superannuation	OPC	Superannuation agencies
Telecommunications Information Privacy Code	Telecommunications	OPC	Telecommunications agencies

Papua New Guinea

Papua New Guinea does not presently provide legislation for the regulation of privacy. However, the Cybercrime Code Act 2016 exists to help regulate activities, crimes and offences, conducted through electronic systems and devices, or in other words, information and communication technologies (ICT). Examples of closely related offences include illegal interception, unauthorised access or hacking and data interference.

Definition of personal data

Personal information has not been defined. However, 'data' has been defined to include any representation of facts, concepts, information (being either text, audio, video, audio-visual or images) machine readable code or instructions, in a form suitable for processing in an electronic system or device, including a program suitable to cause an electronic system or device to perform a function.

Furthermore, 'sensitive data' has been defined to include any data or content whether in writing, images, audio, visual, audio visual or in any other form:

- that is potentially detrimental or damaging to the person who is the subject of such information or personal data; or
- data that is classified or intended for restricted use or specified persons only; or
- data relating to the State, politics and the military, or corporate secrets, or data that is otherwise not available to the public.

Cases

2018 – The PNG government announced intentions to ban its citizens from using an international social media site in order to identify 'fake users' and study the effects which the website has on its population. Communication Minister Sam Basil announced his motivation for the ban, which includes protecting the privacy of PNG's users of the site amidst a global personal information data breach. Basil also highlighted that previous privacy scandals involving the site demonstrate concerning vulnerabilities for PNG citizens and residents on their personal data and exchanges when using social networking sites. However, the concern behind the ban is wider than the potential threat of data breaches themselves from Basil's perspective.

Relevant laws, regulations and standards

Law, regulation and standard	Industry	Regulator	Applicability
Cybercrime Code Act 2016	All	Government	Organisations and individuals
Protection of Private Communications Act 1973	Government	Government	Government agencies

"In a disruptive era of digital transformation, a compliance-centric mindset among personal information controllers and processors would not be enough if our goal is to truly protect the digital Filipino. What we need is to institutionalise a sense of accountability and ethics in the handling of personal data in our organizations."

– Raymund Enriquez Liboro
Privacy Commissioner and Chairman (The Philippines)

The Philippines

In the Philippines, privacy and data protection is governed by the Data Privacy Act of 2012 (DPA), which provides comprehensive protections for personal information. It is supported by the Implementing Rules and Regulations of the Data Privacy Act of 2012. In comparison to its neighbours, the Philippines has one of the stronger privacy regimes in the Asia Pacific region. With a rapidly growing IT, digital economy and population of social media users, the Government and privacy regulator has a mandate to protect the privacy of individuals and ensure the free flow of information.

Primary legislation: Data Privacy Act of 2012

Considerations

- **Extraterritorial jurisdiction:** The Act applies to the processing of personal information belonging to Philippine citizens in and outside of the Philippines, and to organisations that are based in, carry out business in or process personal information collected or held by an entity in the Philippines.
- **Distinguishes between controller and processor:** The DPA distinguishes between 'personal information controller' and 'personal information processor'. The accountability is placed on the controller for personal information under its control or custody, including information transferred to a third party for processing.
- **Provisions specific to Government:** The Act imposes specific requirements for government entities to transmit data to third parties and imposes additional penalties on government officials who breach the Act while carrying out their duties.

Definition of personal information

- Personal information is defined as any information, whether in material form or not, from which the individual can be identified by the entity holding the information, or when put together with other information.
- Sensitive information, which is afforded additional protections, refers to personal information about an individual, such as race, ethnic origin, marital status, age, religion, philosophical or political affiliations, health, education, genetic or sexual life, legal proceeding, criminal history, social security number, health records, tax records, and classified information.

Collection and notice

When collecting personal information, data must be:

- Collected only for a specific and legitimate purpose determined and declared.
- Accurate, relevant and kept up to date where necessary for the declared purpose.
- Adequate and not excessive in relation to the declared purpose.
- De-identified when no longer necessary for the declared purpose.

The data subject is entitled to be informed of:

- The purpose for which the personal information is being collected.
- The scope and method of processing.
- The recipients or classes of recipients to whom personal data will be disclosed.
- Methods to access data.
- The identity and contact details of the data controller.
- The period for which the data will be stored.
- Any rights the data subject may have.

Data subjects shall be notified and given an opportunity to withhold consent in case of any changes to the information declared to the data subject since consent was sought.

Use and disclosure

Personal information must be accurate and relevant. It must only be processed fairly, lawfully, in a way compatible with the declared purpose and in a manner that ensures appropriate privacy and security safeguards. Processing of personal data shall adhere to the principles of transparency, legitimate purpose and proportionality.

Processing personal information is only lawful and permitted where the data subject has consented, or it is necessary:

- For the processor to fulfil a contract with the data subject.
- For the controller to comply with legal obligations.
- To protect the data subject's life and health.
- To respond to a national emergency, uphold public order and safety, or fulfil functions of a public authority.
- As the legitimate interests of the controller or third parties override the data subject's rights.

Sensitive information must not be processed unless the data subject has consented, or it is necessary:

- To fulfil rights or obligations under existing laws and regulations.
- To protect the life and health of the data subject or another person.
- To achieve the lawful and non-commercial objectives of public organisations.
- For purposes of medical treatment, and adequate level of protection is ensured.
- For the protection of lawful rights and interests of individuals.

Consent to the processing of personal and sensitive information must be freely given, specific, informed, and evidenced by written, electronic or recorded means.

Data retention and destruction

Personal data must only be retained for as long as necessary:

- To fulfil the purpose for collection and processing.
- For the purposes of legal proceedings.
- For legitimate business purposes.

Personal data must be disposed securely in a way that does not allow further processing, unauthorised access or sharing to third parties or the public.

The law provides for personal data to be stored and processed for longer periods for historical, statistical or scientific purposes if organisational, physical and technical security measures are implemented. Data that is aggregated and not identifiable may be kept for longer than necessary to fulfil the purposes for which it was collected and processed. Personal data must not be retained for future use where no purpose has been determined.

Security

Controllers must implement reasonable and appropriate organisational, physical and technical measures to protect personal information from accidental or unlawful destruction, alteration, disclosure or processing, natural disasters and human dangers. They should ensure implementation of safeguards to protect their computer network, such as the following:

- A security policy on processing personal information
- Identify and assess reasonably foreseeable vulnerabilities in its networks
- Take corrective mitigating action against security incidents that can lead to a breach
- Regularly monitor security breaches and prevention processes

Sensitive personal information maintained by the Government should be secured as far as practicable, with the use of standards recommended by industry and the Commission.

Individual rights

The data subject is entitled to:

- **Be informed** of what personal information is being processed, purposes for processing, scope and method of processing, retention period, information recipients, identity of the controller, date that the data was last accessed or modified and their rights.
- **Access to personal information:** where the data was collected from, names and addresses of recipients, manner of processing, reasons for disclosure and information about automated data processing where the data will likely be the sole basis for a decision affecting the data subject.
- **Request deletion or suspension of processing** or where the data subject has established that their information is incomplete, outdated, falsely or unlawfully obtained, being used for unauthorised purposes, no longer necessary for the declared purposes, withdraws consent or objects to the processing.
- **Be indemnified for any damage sustained** due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorised use of personal information.
- **Data portability:** the right to obtain a copy of personal data undergoing processing in an electronic or structured form to allow for further use.

Individual rights do not apply where personal information is used only for the needs of scientific and statistical research, and provided that their information is not used to determine decisions regarding the data subject.

Data breach notification

There is a mandatory requirement to notify the National Privacy Commission (NPC) and data subjects in the event of a data breach concerning personal information. The NPC may exempt a controller from notification if it is in the public interest.

All data breaches should be documented through written reports, which include the facts of the incident, effects of the incident and the remedial actions taken by the controller to respond to the breach.

Requirements	
Threshold for reporting	• Controllers must notify the NPC and affected data subjects when sensitive information or other information is: – Likely to enable identity fraud. – Acquired by an unauthorised person. – Likely to give rise to a real risk of serious harm to the data subject.
Time frame	• Within 72 hours of the knowledge of or reasonable belief that a breach has occurred.
Who to notify	• The National Privacy Commissioner. • Affected data subjects.
Content	• Nature of the breach, chronology of events, an estimate of persons affected. • Type of personal data affected. • Remedial steps taken by the controller. • Contact information of a data protection officer that may provide further information to the Commission or data subjects,

Cases

- **2018 –** A fast food company's customer database was accessed by an unknown unauthorised person. The NPC's investigation revealed that the database's protection was not up to date and that some personal information was unencrypted. The NPC ordered the company to: suspend data processing until its security vulnerabilities were addressed, submit a security plan, employ 'privacy by design' in its infrastructure upgrade, conduct a PIA and file a monthly progress report with the NPC until the issues outlined were resolved.
- **2018 –** A social media platform discovered a vulnerability on its website whereby accounts were compromised, exposing personal and sensitive information. The company did not notify users individually as it did not consider the breach as likely to give rise to a real risk of serious harm. It instead notified users about the rectification updates through an in-app message. The NPC considered that a real risk of serious harm was likely to result from the breach. The company was ordered to: submit a more comprehensive data breach report to the NPC, notify data subjects with sufficient details of the breach and risks, provide identity theft insurance and credit monitoring services, establish a help desk for assisting affected data subjects and provide evidence of compliance of the orders.
- **2018 –** A fast food restaurant chain's website was infiltrated, exposing sensitive personal information. The company had not notified affected data subjects at the time that it notified the NPC. They were ordered to: notify affected data subjects and highlight the risk of identity fraud, conduct a privacy impact assessment (PIA), explain to the NPC why it should not take action against the company for its failure to notify the affected data subjects within 72 hours and provide materials to aid the NPC's investigation including its privacy policy and existing security recommendations that had not been implemented before the breach was discovered.

Cross-border data transfer

Private Sector

Before sharing data, controllers must obtain consent from the data subject and provide details of the transfer including relevant data, recipients and the data subject's rights. Consent is required even when the data is to be shared with an affiliate or parent company, or similar relationships.

Data-sharing for commercial purposes, including direct marketing, is to be covered by a data-sharing agreement, which establishes adequate safeguards for data privacy and security. The data-sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject.

Public sector

Data-sharing between government agencies pursuant to a public function or service shall be covered by a data-sharing agreement guaranteeing compliance with the Act, including safeguards for data privacy and security. The data-sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject.

Governance

A data protection officer (DPO) must be designated by controllers and processors engaging in the processing of personal information of individuals if they fall within the territorial scope of the Act.

An organisation may outsource the function of a DPO. However, the designated DPO at the controller or processor remains accountable and must oversee the performance of the outsourced DPO.

Regulators and regulatory landscape

The National Privacy Commission (NPC) is tasked with monitoring compliance with the Act, responding to complaints, investigating incidents, regularly publishing laws relating to data protection, coordinating with regulators in other countries and imposing administrative penalties.

Penalties

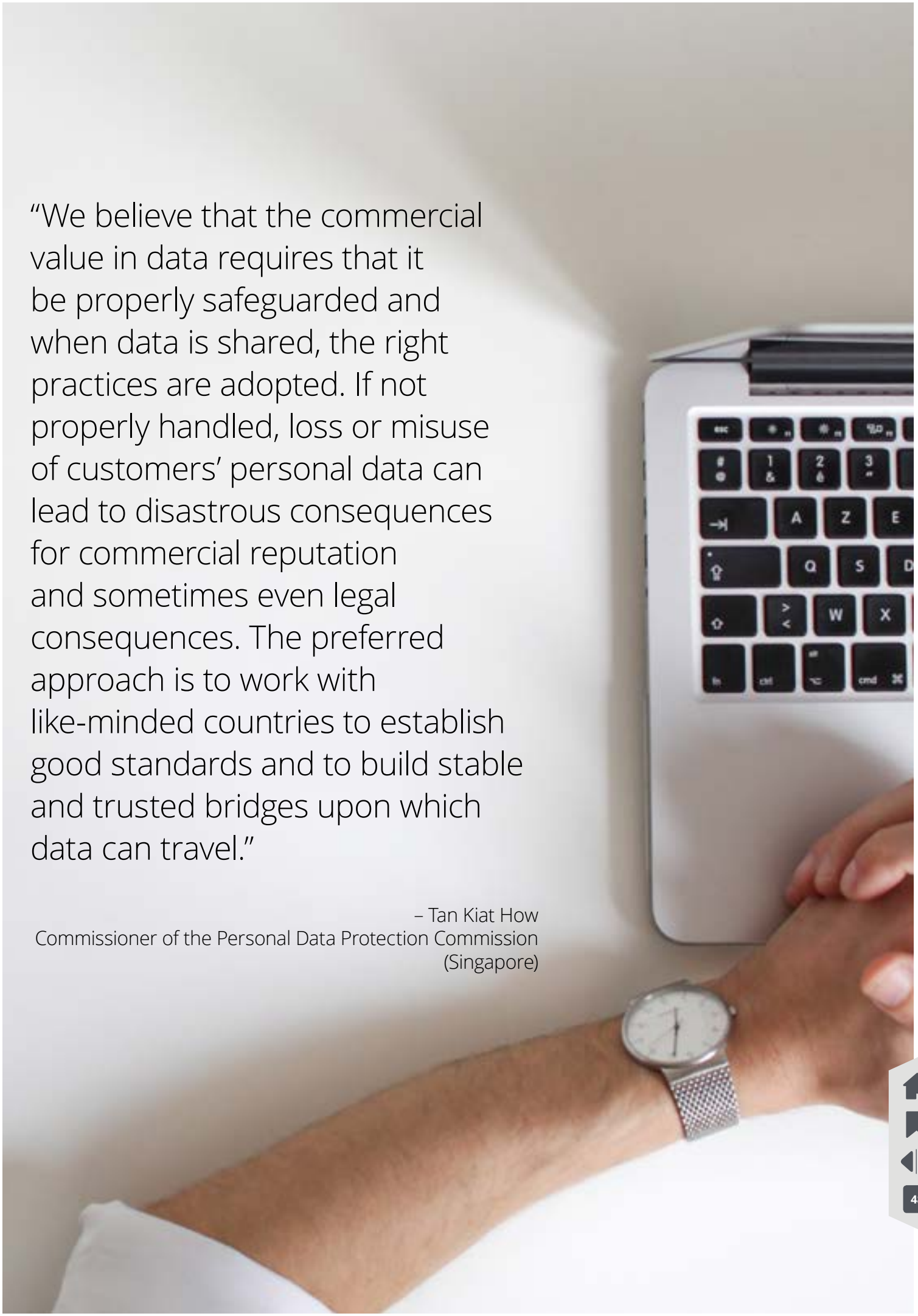
A violation of the data privacy provisions may attract financial penalties and/or terms of imprisonment. For example, the processing of personal information without consent or authorisation under law can lead to a penalty of up to PHP 2,000,000 or a term of imprisonment between one to three years, and PHP 4,000,000 or a term of imprisonment between three to six years for unauthorised processing of sensitive information.

Relevant law, regulation or standard

Law, regulation or standard	Industry	Regulator	Applicability
Implementing Rules and Regulations of the Data Privacy Act	All	National Privacy Commission	Controllers and processors of personal information
NPC Circular 16-01 – Security of Personal Data in Government Agencies	Public sector	National Privacy Commission	Government agencies

Terminology

Terminology	Definition
Consent	Freely given, specific and informed indication of will.
Data subject	An individual whose personal, sensitive personal, or privileged information is processed.
Personal information controller	A person or organisation who controls the collection, holding, processing or use of personal information, or instructs another person or organisation to collect, hold, process, use, transfer or disclose personal information on his or her behalf. Excluding: a person or organisation who is following instructions of another person or organisation and individuals who collect, holds, process or use personal information in connection with the individual's personal, family or household affairs.
Personal information processor	Any natural or juridical person to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
The Rules	Implementing Rules and Regulations of the Data Privacy Act of 2012.



"We believe that the commercial value in data requires that it be properly safeguarded and when data is shared, the right practices are adopted. If not properly handled, loss or misuse of customers' personal data can lead to disastrous consequences for commercial reputation and sometimes even legal consequences. The preferred approach is to work with like-minded countries to establish good standards and to build stable and trusted bridges upon which data can travel."

– Tan Kiat How
Commissioner of the Personal Data Protection Commission (Singapore)

Singapore

As an innovation hub, Singapore is quick to adopt new technologies and has recognised the need to balance an individual's privacy with business innovation. Singapore has a comprehensive privacy framework governed by the Personal Data Protection Act 2012 (PDPA), supported by additional regulations, such as the Personal Data Protection (Enforcement) Regulations and Personal Data Protection Regulations. The public sector is governed by a separate framework that closely follows the PDPA. The Singaporean government is currently in the process of reviewing its current privacy framework and is expected to make amendments to the law, such as the introduction of a mandatory data breach notification requirement.

Primary legislation: Personal Data Protection Act 2012 (PDPA)

Considerations

- **Proposed mandatory data breach notification law:** A mandatory breach notification scheme has been proposed to be introduced through an amendment to the Personal Data Protection Act. There is currently no proposed date for the introduction of the scheme. The intention to introduce a mandatory scheme follows a review of the state of the current laws to address the evolving needs of businesses and individuals after several high-profile data breaches.
- **Data portability:** A discussion paper was released by Singapore's Personal Data Protection Commission and the Competition and Consumer Commission of Singapore detailing the need to facilitate data flows between service providers which will give greater rights to individuals.
- **Data protection in the public sector:** The public sector is subject to similar standards as the private sector. The Public Sector (Governance) Act 2018 and the Government Instructions Manual contain measures to govern protection of personal data, which are aligned with the PDPA.

Definition of personal information

The PDPA defines 'personal data' as data about an individual, living or deceased, who can be identified:

- From that data, or from other data to which the organisation has or is likely to have access to.
- Whether the data is true or not.

The PDPA does not apply to:

- Personal data within a record that has been in existence for at least 100 years.
- Personal data about an individual who has been deceased for more than 10 years.
- Business contact information for business purposes.

Collection and notice

Personal data should only be collected where consent has been provided and it is for a purpose a reasonable person would consider appropriate in the circumstances. The individual must be notified of the purpose of collection.

However, consent is not required where the collection is:

- Necessary for national interest.
- In response to an emergency.
- Necessary for a purpose clearly in the interest of the individual.
- Solely for artistic or literary purposes.

An organisation must make a reasonable effort to ensure that the collected personal data is accurate and complete. This is especially important if the personal data is used by the organisation to make a decision that may affect the individual or it is disclosed to another organisation.

Use and disclosure

Personal data can only be used and disclosed in accordance with the purpose it was collected for and where it is a purpose a reasonable person would consider appropriate in the circumstances. The individual must provide consent for the use and disclosure.

An individual may be deemed to consent for a purpose if they have voluntarily provided personal data for that purpose and it is reasonable that data would be provided in that instance.

Direct marketing

The PDPA applies to all marketing activities, such as electronic marketing, which involve the collection, use or disclosure of personal data. If an organisation conducts any telemarketing activities, they must also abide by the Do-Not-Call (DNC) provisions of the PDPA.

When sending marketing communications to a Singaporean telephone number, an organisation must obtain clear and unambiguous consent from the individual prior to sending the communications. Evidence of the individual's consent must be available for easy reference. When consent is not obtained, organisations must check the telephone number is not listed on the DNC Register, which is managed by the Commission. When contacting individuals, the organisation must identify themselves and provide clear, accurate and up to date contact information. Individuals may apply to the Commission to add or remove their telephone number from the DNC Register.

The PDPA will apply to marketing messages when the sender of the message was or is present in Singapore at the time the message was sent, and when the recipient of the message was or is present in Singapore when the message was accessed.

The Spam Control Act (SCA) regulates electronic marketing activities. This includes the sending of unsolicited commercial communications in bulk, using electronic mail, SMS or MMS.

Data retention and destruction

An organisation must not retain personal data, or ensure steps are taken to de-identify the data, as soon as it can be reasonably assumed that retention of the data no longer serves the purpose it was collected for, or any business or legal purpose.

Although the PDPA does not prescribe specific retention period of personal data, there may be specific industry-standard requirements that may apply.

Security

An organisation must protect personal data, within their possession or control, with adequate and reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure or similar risks. However, the PDPA is not prescriptive in the particular security measures that are required.

Individual rights

Individuals have the right to:

- **Be notified of collection, use or disclosure** of their data for a particular purpose.
- **Withdraw their consent** by giving reasonable notice to the organisation.
- **Access their personal information:** upon request, an organisation must provide access to the individual's information, in addition to details about how the information is used or disclosed, as soon as reasonably possible.
- **Correct their personal information:** upon request, an organisation must correct any error or omission in an individual's data, where that data is in the possession or control of the organisation, and without charging a fee for the correction. If the organisation is unable to correct the personal data within 30 days, individuals should be informed within 30 days.

Data breach notification

There is no mandatory notification requirement for data breaches. However, the Personal Data Protection Commission (PDPC) has provided guidelines for the voluntary notification of data breaches.

In the event of a suspected data breach, an individual may make a complaint to the PDPC or initiate civil action against an organisation.

Voluntary guidance	
Threshold for reporting	• Organisations should conduct an assessment of the breach within 30 days of becoming aware of a potential breach. • Where the breach might cause public concern and where there is a risk of significant harm to a group of individuals.
Time frame	• Organisations are advised to report to the PDPC as soon as practicable and no longer than 72 hours after establishing the breach is likely to result in significant harm to individuals. • If sensitive information is involved, organisations are advised to report immediately.
Who to notify	• Individuals whose personal data may have been affected by the breach. • The PDPC. • Any other third parties affected, e.g. banks, credit card companies, or police.
Content	• Extent of the data breach. • The type of personal data affected. • The amount of personal data affected. • The cause or suspected cause of the data breach. • Steps the organisation has taken to manage the risk and/or rectify the breach. • Information on whether individuals have been notified. • Further steps to be taken by the organisation. • Contact information of a person that affected persons or the PDPC can contact for further information.

Cross-border data transfer

Cross-border data transfer is allowed if the offshore third party has comparable privacy protections in place. This can be achieved by data transfer agreements or consent from the individual. Exemptions to the PDPA may be granted by the PDPC.

Governance

An organisation is required to appoint one or two DPOs to be responsible for ensuring compliance with the privacy laws. The DPO is not required to be a citizen or resident of Singapore, but it is recommended that they are contactable from Singapore, available during Singapore business hours and have a Singapore telephone number. The contact information of the DPO must be publicly available.

Regulators and regulatory landscape

The Personal Data Protection Commission (PDPC) has the power to:

- Prohibit the collection, use or disclosure of personal data that breaches any provision of the Act.
- Destroy personal data that has been collected in breach of the provisions of the Act.
- Refuse the right to access or correct personal data.
- Enforce financial penalties (not exceeding SG $1 million).

Cases

- **2018 –** Hackers stole sensitive health records of 1.5 million hospital patients and 160,000 outpatient prescription records. A financial penalty of SG $250,000 was imposed on the healthcare institution for failing to make reasonable security arrangements to protect personal data.
- **2018 –** A sports association was fined SG $30,000 for unauthorised disclosure of personal data. It was found that the national identification numbers of up to 782 minors was published in a document on the association's website. The identification numbers could be used to identify individuals when the contents were copied and pasted onto another document.

Penalties

A violation of any of the data protection provisions by an organisation can attract a fine of up to SG $1 million. There are further penalties for violations of the Do-Not-Call provisions, which may also attract a term of imprisonment.

Relevant laws, regulations and standards

Law, regulation, standard	Industry	Regulator	Applicability
Computer Misuse Act	All	Commissioner of Police	Individuals and organisations
Cybersecurity Act	Applies to 11 vital sectors, such as energy, information communications, health care and financial services.	Cybersecurity Commissioner	Critical information infrastructure organisations and data users
Personal Data Protection (Composition of Offences) Regulations 2013	All	Personal Data Protection Commissioner	Organisations and data users
Personal Data Protection (Do Not Call Registry) Regulations 2013	All	Personal Data Protection Commissioner	Organisations and data users
Personal Data Protection (Enforcement) Regulations 2014	All	Personal Data Protection Commissioner	Organisations and data users
Personal Data Protection Regulations 2014	All	Personal Data Protection Commissioner	Organisations and data users
Personal Data Protection (Appeal) Regulations 2015	All	Personal Data Protection Commissioner	Organisations and data users
Public Sector (Governance) Act 2018	Public sector	Minister for Communications and Information	Public sector agencies
Spam Control Act 2007	All	Infocommunications Media Development Authority	Organisations

South Korea

As a data-driven economy and world leader in information communications and technology, South Korea has one of the most comprehensive privacy frameworks, which contains principles and policies to protect personal information and provide rights to data subjects.

Privacy is regulated by the Personal Information Protection Act 2011 ('PIPA'), which is comprehensive, principles-based and applies to personal information processors ('processors').

Primary legislation: Personal Information Protection Act 2011

Considerations

- **Embracing technology:** South Korea is embracing and developing technology, such as big data, artificial intelligence, autonomous objects, virtual and augmented realities, IoT and robotics.
- **Global influences:** South Korea aims to align its privacy framework to global standards by seeking the adequacy status from the European Commission to be able to freely transfer information between South Korea and the EU.
- **APEC:** In 2017, South Korea became part of the APEC Cross-Border Privacy Rules System, designed to strengthen regional privacy law enforcement.

Definition of personal information

- Personal information pertains to a living person and can be used to identify an individual. Examples of personal information include a person's name, image or resident registration number. Information will also be considered personal if it can be combined with other information to identify a specific individual.
- Sensitive data includes information such as, and related to, an ideology, belief, membership of a trade union or political party, political mindset, health and sexual life. Sensitive data also includes any other personal information which is likely to cause harm to the privacy of a data subject.

Collection and notice

Personal information can be collected where:

- Consent has been provided by a data subject.
- Required by law.
- Required for the processor to carry out work under laws and regulations.
- Necessary to execute and perform a contract with the data subject.
- Necessary for the protection of the data subject or a third party, such as a legal representative, from danger to life, body or economic profits.

Processors must establish a personal information processing policy, such as a privacy policy, and disclose it to data subjects as well as making it available for public access.

When obtaining consent, data subjects must be provided with notice of the following, including where modified, in an explicitly recognisable manner:

- Purpose of and use for collection.
- Types of information collected.
- Period for use and retention.
- Right to refuse consent and any implications arising from refusal.

Use and disclosure

Processors must process personal information:

- In a lawful and fair manner.
- In accordance with the specified and intended purpose.

Provided the information is unidentifiable and consent was provided for an intended purpose, exceptions apply where:

- The purpose is likely to infringe upon the data subject's interests.
- It is required for legal proceedings or used as part of statistics and/or academic research.

Provided the information is unidentifiable and consent was provided for that purpose.

Personal information must be used with the aim to:

- Minimise the possibility of infringing the data subject's rights.
- Maintain trust between data subjects.

Sensitive data

Sensitive data cannot be processed unless:

- Explicitly required or permitted by laws and regulations; or
- Consent has been obtained

Direct marketing

Data subjects must be notified if personal data will be used to promote or sell goods or services.

Individual rights

Data subjects have the right to:

- **Be informed** of their rights and how the information will be used.
- **Request access, correction and erasure** to their personal information.

Data retention and destruction

Personal information must be kept up-to-date, complete and accurate. If the processor is required by law to retain the information, they must store and manage that particular information separate from other personal information.

Processors must destroy the information without delay once the intended purpose has been fulfilled or when the information is no longer necessary.

Security

Processors must prevent personal information from loss, theft, forgery, disclosure, alteration, damage and destruction by implementing technical, managerial and physical measures, such as:

- Controlling access and restricting authority to access
- Adopting encryption technology
- Installing, maintaining and upgrading security programs, storage and locks
- Developing an internal management plan
- Preserving log-on records

Data breach notification

Data breach notification is a requirement which processors must adhere to, as provided by the PIPA.

Requirements	
Threshold for reporting	• Processors must notify the Minister of Public Administration and Security (MPAS) and aggrieved data subjects once becoming aware that personal information has been leaked.
Time frame	• Processors must provide notification without delay. This is interpreted to be "within five days" under regulatory guidance, except for certain sectors that provide their own specific reporting requirements. For example, information and communication service providers ('ICSP') must notify the Communications Commissioner within 24 hours.
Who to notify	• MPAS • Aggrieved data subjects
Content	• Notification must include: – The kind of information leaked – When and how the information was leaked – Remedies which can be undertaken by the data subject to minimise damage – Countermeasures and remedial procedures to be undertaken by the processor – Details for contact points, such as a help desk, to report damage

Cross-border data transfer

Personal information can only be shared with third parties where any one of the following conditions has been satisfied:

- Where consent has been provided by a data subject.
- Where required by law.
- Where required for the processor to carry out work under laws and regulations.
- Where necessary to execute and perform a contract with the data subject.
- Where necessary for the protection of the data subject or a third party, such as a legal representative, from danger to life, body or economic profits.

When transferring personal information to third parties, processors must inform the data subject of the recipient, purpose for sharing, type of personal information shared, period of use and retention, and individual rights.

For the purposes of transferring personal information across borders, processors must obtain explicit consent from the data subject and must not enter into contracts contrary to the PIPA.

Governance

The processor concerned must designate a privacy officer, who is responsible for:

- Protecting, controlling and managing personal information
- Establishing and implementing personal information protection plans
- Surveying processing practices and improve shortcomings regularly
- Managing complaints
- Building internal controls systems
- Preparing and implementing education programmes
- Taking and reporting immediate corrective measures, if necessary.

Regulators and regulatory landscape

The Personal Information Protection Commission (PIPC) is the primary regulator for privacy within South Korea.

The PIPC is responsible for:

- Protecting personal information.
- Ensuring personal information is fairly collected and legitimately processed.
- Monitoring data protection violations.
- Mediating to redress damage caused by violations.
- Ensuring data protection laws are properly interpreted and applied.

Cases

- **2014 –** A travel agency used personal information for commercial purposes without the data subject's consent and was ordered to pay ₩300,000 as compensation for mental distress, and advised to provide an educational program to employees about personal information of customers.
- **2015 –** After completing a consent form for his spouse, Mr X discovered that the hospital collected his resident registration number, which was prohibited under the PIPA, unless specifically permitted by a relevant law or for urgent needs of the data subject, Mr X, or a third party. The hospital was required to correct its consent form to conform with the PIPA and implement a plan to prevent reoccurrence through privacy awareness educational programmes.

Penalties

Fines of up to ₩100 Million and imprisonment of up to 10 years may be issued as punishment for breaches within the Act primarily by the Ministry. However, other bodies, including the PIPC, may undertake enforcement activities.

For data breaches caused by intentional or negligent violations of information and communications services providers, data subjects may claim compensation of up to ₩3Million.

Relevant Laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Act on the Development of Cloud Computing and Protection of its Users 2015	All	Minister of Science, ICT and Future Planning	Commercial cloud computing service providers
Act on Promotion of Information and Communications Network Utilization and Information Protection 2001	Information and Communication	Korean Communications Commission (KCC)	Information and communications service providers
Act on the Protection and Use of Location Information 2010	All	KCC	Location information businesses
Credit Information Use and Protection Act 1995	Financial services	Financial Services Commission	Credit information providers
Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection	Telecommunications	KCC	Information and communications service providers
Enforcement Decree of the Personal Information Act (Presidential Decree No.28355)	All	Ministry of the Interior and Safety, Personal Information Protection Commission (MISPIPC)	Data controllers and processors
Personal Information Protection Act 2011	All	MISPIPC	Data controllers and processors

Terminology

Terminology	Definition
Data subject	An individual identifiable by/the subject of information processed.
Information and communications services providers	Licenced telecommunications business operators and other persons who provide information or act as an intermediate to provide information commercially by utilising services provided by a telecommunications business operator.
Personal information processor	Public institutions, legal persons, organisations or individuals that process personal information directly or indirectly for official or business purposes.
Processing	The collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, retrieval, output, correction, recovery, use, provision, disclosure or destruction of personal information and other similar activities.
Sensitive data	Information pertaining to data subjects' ideology, belief, trade union / political membership, political opinions, health, sexual life or other personal information likely to infringe privacy.

Sri Lanka

There is a growing need to protect personal information for individuals in Sri Lanka with an increasing population that is able to access the internet and social media. Sri Lanka does not currently have a specific privacy regime, however there are a number of laws in place to govern the use of electronic records and communications. Although the Sri Lankan Constitution does not provide explicit reference for a right to privacy, the Telecommunications Minister has confirmed that a Data Privacy Act will be introduced to Parliament in 2019.[9]

Considerations

- **Digital identities:** A national digital identity scheme, incorporating electronic identity cards and passports, concerning primarily biometric data, was launched in 2019 to enable citizens to transact securely online, help prevent identity fraud and other related scams.
- **Internet and social media use:** Currently, 34% of the population use the internet. This amounts to 7.13 million people, of which 6.2 million are active social media users. As social media use increases, the need for greater governance is also required. It is not uncommon for access to social media to be blocked.
- **Privacy reform:** The ICTA is looking to adopt a data protection code of practice under the existing Information Communication Technology Act 2003. However, no timeframe has been provided for when this will occur. There are also plans to enact a Cyber Security Act and a Data Protection Act (DPA) while also establishing a high level security agency for Sri Lanka and empowering the Sri Lanka Computer Emergency Readiness Team (SLCERT) within 2019.

Regulators and regulatory landscape

The Information and Communication Technology Agency (ICTA) is responsible for:

- Overseeing e-laws and helping to regulate electronic data and documents within electronic transactions; and
- Implementing data protection policies for the future

[9] https://economynext.com/Sri_Lanka_data_privacy_bill_to_parliament_in_three_months-3-13895-10.html

Relevant laws

Law	Coverage/ industry	Regulator	Applicability
Computer Crimes Act 2007	Cybercrimes	Minister in charge of Science and Technology	Data subjects
Electronic Transaction Act 2006	Electronic contracts and certification services	N/A	Originators and addressees
Information and Communications Technology Act 2003	All	ICTA	ICTA
Right to Information Act 2016	All	Right to Information (RTI) Commission	Citizens
The Telecommunication Act 1996	Telecommunication transmissions	Telecommunication Regulatory Commission of Sri Lanka	Telecommunications officers and operators

Terminology

Terminology	Definition
Addressee	The person intended by the originator to receive the communication.
Citizen	A body, whether incorporated or unincorporated.
Operator	A person authorised by license to operate a telecommunication system.
Originator	A person, by who or on whose behalf, the communication purports to have been sent or generated prior to receipt or storage.
Telecommunications officer	Any person employed, permanently or temporarily, in connection with any telecommunication service provided by an operator.

Taiwan

In Taiwan, personal information is protected under the Personal Information Protection Act (PIPA) and is enforced by industry regulators and local government authorities. The law applies to private entities as well as government bodies.

When drafted, the PIPA considered the European Union Data Protection Directive (Directive 95/46/EC). Taiwan recently joined the Asia-Pacific Economic Forum's Cross Border Privacy Rules system, making it only the 7th APEC member to do so.

Primary legislation: Personal Information Protection Act

Considerations

- **Increasing discourse and public awareness of privacy rights:** The Ministry of Justice is currently considering the interaction of privacy rights and big data. Even though the benefits of big data have been recognised, there is a struggle to balance the increasing awareness of privacy rights and the desire to control how personal information is being used by organisations. There is ongoing debate regarding whether data subjects have the right to opt out of having their de-identified information used by organisations to perform analysis.
- **GDPR:** The extra-territorial reach of GDPR has, as with many other countries, a significant effect on businesses in Taiwan. Taiwanese exports to the EU amounted to US$7.07 billion in the first quarter of 2018, and imports from the EU amounted to US$7.64 billion. As such, there is a significant relationship with European businesses. In particular, the technology industry will need to re-examine their privacy laws to ensure a similar standard is upheld.
- **Establishment of Personal Data Protection Office:** In 2018, the National Development Council established the Personal Data Protection Office. The focus of the office will be to address GDPR issues and coordinate with the relevant authorities. It is also working towards obtaining an adequacy decision from the European Union for having an adequate level of protection for cross-border transfer of personal data between the EU and Taiwan.

Definition of personal information

- Personal information is defined as any information that may be used to identify a natural person, directly or indirectly. It includes: the name, date of birth, ID card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions and social activities.
- The PIPA recognises a special category of personal information that must not be collected, processed or used, which includes medical records, medical treatment, genetic information, sexual life, health examination and criminal records. However, there are exceptions that may apply in limited circumstances.

Collection and notice

Personal information should only be collected if it is:

- Respectful of the rights and interests of the data subject
- Following the principle of 'bona fide'
- Reasonable and fair
- Limited to the purpose of collection

When collecting personal information, the organisation is required to inform data subjects of the organisation's name, purpose of collection, classification of data, uses of data, the data subject's rights and consequences if they choose not to provide the personal information.

Use and disclosure

Personal information must only be used by businesses if it is in compliance with the specific purpose of collection, and should comply with one of the following:

- It is in accordance with law
- There is a contract or a quasi-contract with the data subject
- Voluntarily provided by the data subject or the data has been lawfully made public
- Used for research by an academic research institution or used for public interests on statistics by a government agency (however, the information must be de-identified)
- Consent has been obtained
- Does not harm the rights and interests of the data subject

Government agencies must only process personal information for a specific purpose and in compliance with at least one of the following:

- Consent has been obtained
- Does not harm rights and interests
- Processing is within scope of job functions provided by laws and regulations

However, there are specific exceptions to the above processing requirements for agencies, such as if processing is necessary for public interest or to prevent harm on rights and interests of other people.

When disclosing to third parties, organisations are required to ensure the protection of personal information. If information is shared to third parties, the organisation and third party are both liable for data breaches by the third party.

Direct marketing

Direct marketing may only be conducted with consent, and an opt-out mechanism must be in place should the user no longer wish to take part. Individuals must be informed of their right to object to use of their personal information for marketing purposes.

Data retention and destruction

Personal information may be retained while the purpose of processing or use exists, or during the term of use. The information can be retained after this period if consent is provided in writing, it is necessary for performance of job duties or legally required.

Security

Agencies must ensure the security of personal data to prevent it from being stolen, altered, damaged, destroyed, lost or disclosed. Some guidance is provided in the PDPA Enforcement Rules for considerations to be made for security measures, such as mechanisms to evaluate risk and manage personal data, mechanisms to respond to data breaches, internal procedures for collection, processing and use of data, information security and personnel, and education and training.

Individual rights

Data subjects have the right to:

- **Access** their data: including review, copy and add to or correct their data. The organisation is obligated to do this unless there is a national security concern, it is a statutory duty for a government agency, or there is material interest of the data processor or third party.
- **Object** to processing of their data: They can ask the organisation to cease collection, processing and use of data.
- **Request deletion** of data: if the purpose for processing no longer exists, data subjects can request their data be deleted, unless it is necessary for a government agency's function, or the individual consents to their data being retained.
- **Make a complaint** to data protection authorities about misuse of their personal information.

Data breach notification

While there is no requirement under the PIPA to notify the regulator for breaches of personal information, there are notification requirements under sectoral laws including for the government, financial and telecommunications sectors.

Under the PIPA, there is a mandatory requirement to notify data subjects affected by a data breach.

Requirements	
Threshold for reporting	• If a data breach has occurred, the breach must be investigated and reported to the data subject by mail, email, fax, or in an advertisement. • There is no requirement to inform any regulator of a data breach occurring under the PIPA. Note, that regulators may require notification separately: – Financial Supervisory Commission requires organisations to notify in case of a breach that may affect business operations or many customers. – Ministry of Health and Welfare requires notifications if there is a breach related to biobanks. – Ministries of the Interior and Economic Affairs also have notification requirements.
Time frame	• No strict time frame – after investigation of the incident.
Who to notify	• Affected data subjects. • Regulator is not required to be notified.
Content	• The occurrence of a data breach. • Steps that have been taken by the organisation or government agency to resolve the incident.

Cross-border data transfer

Cross-border transfers are generally permitted. There are no data transfer agreement requirements. However, the following exceptions apply:

- Biological specimens in a biobank
- International transmission of biobank data must be approved by the relevant authority
- Financial Supervisory Commission approval is required to outsource retail operations
- Telecommunications providers cannot transfer data to China

If one of the following has occurred when the non-government agency transmits personal information internationally, the government authority in charge of the subject industry may limit its action where:

- It involves major national interests.
- National treaty or agreement specifies otherwise.
- The country receiving personal information lacks proper regulations towards the protection of personal information and it might harm the rights and interests of the party.
- International transmission of personal information is made through an indirect method in which the provisions of this law may not be applicable.

Governance

Agencies are not required to appoint a data protection officer. However, government agencies are required to hire personnel for the security and maintenance of files.

Regulators and regulatory landscape

There is no single regulatory agency to oversee and enforce the provisions of the PIPA. However, the Ministry of Justice is tasked as the drafting and interpreting agency of the PIPA in order to provide guidance for other supervisory agencies and regulators to enforce the provisions.

Cases

- **2017 –** The FSC investigated an insurance agency that mailed personal information to third parties unintentionally, and found that this was caused by errors in the software used to send notices. A penalty was given (NT$50,000 for the organisation and responsible party) for failure to report the breach in the required timeframe.
- **2017 –** An insurance agency was found to be non-compliant, being penalised by the FSC for failure to inform data subjects in accordance with notification requirements when collecting their information.
- **2018 –** A large bank was fined NT$2,000,000 by the FSC for a data breach caused by a failure in the internal control system to maintain information security, which allowed for administrator access to be broad and not properly managed.

Penalties

Regulatory bodies are able to enforce the PIPA on private sector organisations by ordering them to remedy violations. If this does not occur, administrative fines up to NT$200,000 may be imposed. Criminal sanctions may be imposed in exceptional cases, such as where a person makes an unlawful profit for himself or a third party by illegally changing or deleting personal information files. This violation may attract imprisonment of up to 5 years or a fine of up to NT$1,000,000, or both.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Act Governing Electronic Payment Institutions	Banking and Finance	Financial Supervisory Commission	Electronic payment institutions as defined under the Act
Employment Service Act	All	Ministry of Justice	All
Financial Holding Company Act	Banking and Finance	Financial Supervisory Commission	Banks, insurance companies and securities firms under the Act
Freedom of Government Information Law	Public sector	Ministry of Justice	Government agencies disclosing personal information
Human Biobank Management Act	Medical and Sciences	Ministry of Health and Welfare	Biobank operators
Medical Care Act	Medical	Ministry of Health and Welfare	Any institution in which physicians conduct the practice of medicine
Pharmaceutical Affairs Act	Medical and Sciences	Ministry of Health and Welfare	Pharmaceutical organisations

Terminology

Terminology	Definition
Data users	Person or public/private legal entity that controls collection, storage, processing or use of personal data.
Data processing	Actions to record, input, store, compile, correct, duplicate, retrieve, delete, output, connect or internally transmit information to establish or use a personal information file.
Data use	Any other personal information use not defined under data processing.
Government agency	Agency or administrative juridical person at central or local government level which may exercise sovereign power.
Non-government agency	All persons, juridical persons or groups other than those that are government agencies.
Organisation	Refers to any non-government agency or government agency.

Thailand

After much anticipation, and nearly a decade of proposed privacy legislation being on the agenda, the Personal Data Protection Act is now effective from 27 May 2019. Organisations will be given one year to become compliant with the legislation. This legislation will provide a comprehensive framework for privacy governance, with themes largely drawn from the GDPR.

Thailand also has sector-specific privacy laws and regulations which provide protection for specific types of information, such as credit information.

Primary legislation: Personal Data Protection Act

Considerations

- **Extraterritorial reach:** Data controllers and data processors will be subject to the PDPA where their processing activities relate to the offering of goods or services, or monitoring of behaviour of data subjects in Thailand, even where the controller or processor is not located in Thailand.
- **Government surveillance:** The National Legislative Assembly has also recently approved a draft Cybersecurity Act that provides obligations for organisations to protect information, particularly organisations dealing with critical information infrastructure. It aims to address cyber threats and national security.
- **Digitisation:** The current vision for Thailand's economic growth, called 'Thailand 4.0', pushes for a move towards a digital economy. Part of this initiative involves amending the Electronic Transaction Act for e-signatures and a Digital ID Bill for digital authentication.

Collection and notice

Collection of personal data should be restricted to data that is necessary, lawful and relevant to the activities of the data controller.

The collection of sensitive data without consent is prohibited, unless it is:

- Necessary to prevent harm to life, body or health.
- Necessary to comply with laws for public interest in health care or labour protection.

Before or at the time of collection, the data controller must provide notification to individuals. Notification must include: the purpose of collection, the type of personal data collected, period of retention, who personal data may be disclosed to, rights of the data subject and contact information of the data controller.

Definition of personal data

- The PDPA defines personal data as any data that can directly or indirectly identify a living person.
- 'Sensitive data' is recognised as a special category of personal data with additional protections. It includes data relating to ethnicity, race, political opinions, religious or philosophical beliefs, sexual behaviour, criminal records, health records, genetic data, labour union membership and biometric data.

Use and disclosure

Personal data must only be used for the purpose or purposes it was collected. In addition, a data controller must receive consent from a data subject for the use or disclosure of their information. Consent must be express and given in writing or through electronic means. Consent is not required where use or disclosure of personal data is:

- For a benefit relating to planning, statistic or making consensus by government agencies.
- For the benefit of investigation by officials in accordance with law.
- To prevent danger to a person's life or health.
- Data that has been lawfully disclosed to the public.
- Prescribed by law, court or Ministerial Regulation.
- Third parties receiving personal data from data controllers can only use or disclose the data in accordance with the purpose or purposes given at the point of collection.

Data retention and destruction

Personal data must be destroyed when:

- No longer legally required to be retained;
- It is no longer relevant or necessary for the purpose of collection; or
- The data subject has withdrawn consent.

However, destruction is not required under certain conditions, such as where it is kept to prove a legal claim, or it is necessary for freedom of information, public interest or compliance with a legal obligation.

Individual rights

Data subjects have the right to:

- **Be informed** of their rights prior to the collection and use of their data.
- **Request** access to their personal data
- **Data portability:** data subjects can ask for a copy of their data in a widely used format such that it may be processed in an automated method, unless it is not technically feasible.
- **Request erasure** when the controller does not comply with PDPA. Data subjects can request that their personal data be deleted, destroyed, temporarily suspended or anonymised.

Security

An organisation must implement appropriate security measures to prevent loss, unauthorised access, use, alteration or disclosure of personal data. The security measures must be reviewed when necessary or when technology changes to ensure appropriate level of security is maintained.

Data breach notification

Under the PDPA, there is a mandatory requirement to report data breaches to the Personal Data Protection Committee (PDPC) and notify data subjects. The PDPC has yet to publish guidance on the reporting of data breaches.

Further, certain sectors and industries have specific notification requirements, such as for electronic payment service providers and telecommunication operators.

Data transfer

A controller can only transfer personal data to foreign countries when:

- The PDPC has determined that the country or organisation has adequate personal data protection measures (to be defined by the PDPC).
- The transfer complies with cross border transfer guidance provided by the PDPC.

However, there are exceptions, such as where the transfer:

- Of personal data is required by law.
- Has been consented to by a data subject and they have been informed of the receiving country's lack of adequate privacy protections.
- Is necessary for the performance of contract.
- Is in accordance with an agreement between a controller and another entity for the benefit of a data subject.
- Is necessary to prevent damage to life, body, or health of the data subject or other persons.
- Is necessary for substantial public interest purposes.

Governance

Data controllers and processors are required to appoint a data protection officer (DPO) when:

- Collection, use or transfer of personal data involves regular monitoring of personal data or systems, i.e. most organisations with an online presence.
- Personal data is processed on a large scale.
- Their core activities involve processing of sensitive data.

Regulators and regulatory landscape

The Personal Data Protection Committee's (PDPC) roles and responsibilities will involve tasks such as preparing a strategic plan to promote data protection, providing advice on compliance with the law, performing prescribed duties under the law, prescribing measures or guidelines, interpreting and deciding on issues, enforcing the law and imposing penalties.

In addition, there will be a supporting body acting as an expert committee. Their roles and responsibilities involve tasks such as considering complaints made under the PDPA, investigating alleged violations, mediating disputes, performing prescribed duties under the law, imposing administrative penalties, and issuing orders to controllers or processors for remedial action.

Cases

- **2018** – The identity documents of around 45,000 customers of a mobile network were found to be stored on a public-facing storage service. The Thai National Broadcasting and Telecommunications Commission ordered the company to compensate customers for damage suffered as a result, in accordance with civil and criminal laws.
- **2018** – Two major banks reported that a total of 123,000 customers had their data stolen by cyber attackers. Following this incident, the Bank of Thailand instructed all Thai banks to focus on uplifting cyber security policies and create compensation regimes for financial damage stemming from data breaches.

Penalties

Non-compliance with the PDPA can amount to:

- Administrative fines (up to THB 5 million).
- Criminal penalties for directors held personally liable for non-compliance (imprisonment up to one year and/or fines up to THB 1 million).
- Punitive damages.

Example of penalty: The unlawful collection of personal data causing damage to another person may attract a penalty of up to THB 300,000 and/or 6 months imprisonment for the individual responsible.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Regulator	Applicability
Broadcasting and Television Business Operation Act 2008	Telecommunications	National Telecommunications Commission	Sound and television broadcasting businesses
Credit Information Business Act 2002	Financial	Credit Information Protection Committee	Credit information companies, data controllers and processors
Financial Institutions Act 2008	Financial	Ministry of Finance	Financial businesses
Notification on the Electronic Transactions Commission on Policy and practice Statement on Personal Data Protection of a Government Agency B.E. 2553 2010	Public sector	N/A	Government agencies
Official Information Act 1997	Public sector	N/A	State agencies
Telecommunications Business Act 2001	Telecommunications	National Telecommunications Commission	Licensed telecommunication businesses

Terminology

Terminology	Definition
Data controller	Natural or legal person that solely, or jointly, are responsible for information processing.
Data processor	Natural or legal person that processes information on behalf of an information controller.

Vietnam

Vietnam does not have a comprehensive legislative regime or regulatory body responsible for privacy. There are varied requirements relating to the protection of personal information across a number of laws.

The Law on Network Information Security (86/2015/QH13) ('NIS Law'), also widely referenced as the Law on Cybersecurity, establishes the most comprehensive requirements and definitions regarding the protection of personal information. These requirements apply to individuals and organisations engaged in information technology application and development activities.

There are a number of laws and regulations that apply to certain sectors and types of transactions, such as the Law on Protection of Consumers' Rights, the Law on Information Technology and the Decree on E-Commerce, which may apply to personal information.

Primary legislation: Law on Network Information Security (86/2015/QH13) ('NIS Law')

Considerations

- **Increased priority for cyber security.** In 2018, Vietnam enacted the Law on Cybersecurity (24/2018/QH14), which increases the power granted to the State to investigate users and censor content published online by individuals.
- **Data localisation.** The NIS Law establishes stricter requirements for foreign service providers operating in Vietnam, including data localisation in certain circumstances. Businesses that collect and process the personal data of Vietnamese citizens are required to maintain a physical office and store the data in Vietnam.

Collection and notice

The NIS Law requires that when collecting personal information, organisations and individuals must collect personal information only after obtaining the consent of the information owner on the scope and purpose of the information collection and use.

Definition of personal data

- Personal information is defined broadly by the NIS Law as information relating to the identity of a specific person. The personal information owner is the person identified by the personal information.
- There is no specific definition of sensitive information under this law. However, certain definitions of personal information found in alternate laws do reference specific types of information as requiring protection. For example, the Decree on E-Commerce extends to 'information contributing to identifying a particular individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that the individual wishes to keep confidential.'

Use and disclosure

The NIS Law requires that when collecting or using personal information, organisations and individuals must only use collected personal information for any purpose different from the initial one only after obtaining the personal information owner's consent.

They must not share or disclose personal information to any third party, unless it is agreed by the personal information owner or requested by competent state bodies.

Data localisation

The NIS Law includes a requirement for domestic and foreign service providers who process personal information of service users in Vietnam to store data locally.

The supporting Draft Decree clarifies that the service providers that may potentially be subject to data localisation can include services relating to social media, email, online payments, online games and telecommunications.

Direct marketing

The NIS Law prohibits organisations and individuals from sending commercial information to a recipient's electronic address without his/her prior consent, request, or when the recipient refuses it, except for the cases where the recipient is obliged to receive the information under current laws.

The Law on Protection of Consumers' Rights also includes a prohibition on the harassment of consumers through the marketing of goods and services contrary to the wishes of the consumer.

Individual rights

The NIS Law provides that individuals shall have rights to access their personal information being collected, handled or stored by an organisation or individual.

Data security

Organisations are required to take appropriate managerial and technical measures to protect personal information that is collected and stored; and that remedial action is taken to mitigate risks to that personal information.

There is also a requirement for information systems to be classified in accordance with a rating between 1 and 5, based on the impacts likely in the event of sabotage to the system.

Cross-border data transfer

There are no specific restrictions on the cross-border transfer of personal information in Vietnam. However, the Law on Cybersecurity requires that organisations must not share personal information to any third party, unless it is agreed by the individual or requested by competent state bodies.

There are no specific restrictions or requirements in Vietnam which apply to cross-border transfers of personal information.

Regulators and regulatory landscape

There is no dedicated privacy or data protection regulator in Vietnam. The Ministry of Information and Communications is primarily responsible for the NIS Law, but may work in conjunction with other departments relating to other information technology and e-commerce laws.

The Ministry of Information and Communications responsibilities extend to the regulation of the press, publishing, posts, telecommunications, information technology, electronics, broadcasting, media, foreign information, domestic and national information, communication infrastructure and management of related public services on behalf of the Government.

Cases

2016 – An airline's website was hacked compromising the personal information of 410,000 clients. The information included names, addresses and birth dates. Following the incident, the airline updated its external privacy notice on its website to state that the company will follow the provisions of the European Union's General Data Protection Regulation (GDPR) and contact affected individuals in the event of a data breach. The airline has also now appointed a data protection officer.

Data breach notification

Data breach notification to a regulator or data subjects is not mandatory. Limited guidance has been provided which can be found in the table below.

Voluntary guidance	
Threshold for reporting	Data breach reporting is required 'in the case that an information system is hacked, posing a risk of loss of consumer information'.
Time frame	The Decree on E-Commerce requires that, 'information storing units shall notify the incident to a functional agency within 24 hours after detecting it.'
Who to notify	The Ministry of Industry and Trade, in conjunction with the Ministry of Information and Communications are responsible for the Decree on E-Commerce.
Content	There is no specific requirement relating to the content to be included in notifications.

Relevant laws, regulations and standards

Law, regulation or standard	Industry	Responsible ministry	Applicability
Decree on E-Commerce (52/2013/ND-CP)	All	Ministry of Industry and Trade	Organisations and individuals conducting part or the whole of the process of commercial activity by electronic means connected to the internet, mobile telecommunications network or other open networks
Law on Cyber Security (24/2018/QH14)	All	Cybersecurity Task Force, under the Ministry of Public Security	Vietnamese and foreign enterprises which provide services on telecom networks and on the internet and other value added services in cyberspace, in Vietnam
Law on Information Technology (67/2006/QH11)	All	Ministry of Information and Communications	Vietnamese and foreign organisations and individuals engaged in information technology application and development activities in Vietnam.
Law on Network Information Security (86/2015/QH13)	All	Ministry of Information and Communications	Any Vietnamese agencies organisation, individual; foreign organisation and individual in Vietnam who directly involves in or is related to network information security activities in Vietnam.
Law on Protection of Consumers' Rights (59/2010/QH12)	All	Ministry of Trade and Industry	Consumers; organisations or individuals trading goods, services; agencies, organisations or individuals involved in activities to protect the interests of consumers in the territory of Vietnam

Comparison matrix

The table below provides a visual comparison of selected privacy elements covered across the Asia Pacific region.

Location	Definition of personal information/data		Collection and notice	Use and disclosure	Data retention and destruction	Individual rights				Security	Data breach notification		Data transfer	Data protection officer
	Personal	Sensitive				Request access	Right to be forgotten	Request suspension of processing	Data Portability		Mandatory	Voluntary Guidance		
Australia	✓	✓	✓	✓	✓	✓	×	×	×	✓	✓	✓	✓	×
Brunei Darussalam	✓	×	✓	✓	✓	×	×	×	×	✓	×	×	✓	×
Cambodia	×	×	×	×	×	•	×	×	×	×	×	×	×	×
China	✓	×	✓	✓	✓	×	×	×	×	✓	✓	✓	✓	×
Hong Kong	✓	×	✓	✓	✓	✓	×	×	×	✓	×	✓	✓	×
India	✓	✓	✓	✓	✓	✓	•	•	•	✓	✓	✓	✓	•
Indonesia	✓	×	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×
Japan	✓	✓	✓	✓	✓	✓	×	✓	×	✓	×	✓	✓	×
Lao PDR	✓	×	✓	✓	✓	✓	×	✓	×	✓	×	×	✓	×
Malaysia	✓	✓	✓	✓	✓	✓	×	×	×	✓	•	×	✓	×
Mongolia	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×
Myanmar	×	×	×	×	×	×	×	×	×	×	×	×	×	×
New Zealand	✓	×	✓	✓	✓	✓	×	×	×	✓	•	✓	✓	✓
Papua New Guinea	×	×	×	×	×	×	×	×	×	×	×	×	×	×
The Philippines	✓	✓	✓	✓	✓	✓	×	×	•	✓	✓	✓	✓	✓
Singapore	✓	×	✓	✓	✓	✓	✓	✓	•	✓	•	✓	✓	✓
South Korea	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Sri Lanka	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Taiwan	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×
Thailand	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×	✓	✓
Vietnam	✓	×	✓	✓	×	✓	×	×	×	✓	×	×	×	×

Key:

✓ The law addresses this element

× There is no law that addresses this element

• It is proposed within a draft Bill, but the law is not yet enacted and in force

Regulatory landscape table

The table below provides at a glance the privacy regulatory landscape of locations across the Asia Pacific.

Location	Regulation	Constitutional right to privacy	Regulator	Maximum penalty for privacy law breach
Australia	Comprehensive	No	Office of the Australian Information Commissioner	Financial penalty (up to AU $2.1 million) and enforceable undertakings
Brunei Darussalam	Sectoral	No	Minister at the Prime Minister's Office	None
Cambodia	Sectoral	Yes	None	None
China	Information security law	Yes	Cyberspace Administration of China	Personal liability and/or criminal sanctions
Hong Kong	Comprehensive	Yes	The Office of the Privacy Commissioner for Personal Data	Personal liability and/or criminal sanctions
India	Information security law	Yes	Non-privacy specific	Personal liability and/or criminal sanctions
Indonesia	Information security law	Yes	Ministry of Communication and Information Technology	None
Japan	EU adequacy	Yes	Personal Information Protection Commission	Personal liability and/or criminal sanctions
Lao People's Democratic Republic	Information security law	No	Ministry of Posts and Telecommunications	None
Malaysia	Comprehensive	No	Personal Data Protection Department and Malaysian Communications and Multimedia Commission	Personal liability and/or criminal sanctions
Mongolia	Sectoral	Yes	Non-privacy specific	None
Myanmar	Sectoral	Yes	Ministry of Communications and Information Technology	None
New Zealand	EU adequacy	No	Privacy Commissioner's Office	Financial penalty (up to NZ $350,000) and codes of practice
The Philippines	Comprehensive	Yes	National Privacy Commission	Personal liability and/or criminal sanctions
Papua New Guinea	Information security law	Yes	None	None
Singapore	Comprehensive	No	Personal Data Protection Commission	Personal liability and/or criminal sanctions
South Korea	Comprehensive	Yes	Personal Information Protection Commission	Personal liability and/or criminal sanctions
Sri Lanka	Information security law	No	Information and Communication Technology Agency	None
Taiwan	Comprehensive	Yes	Personal Data Protection Office	Personal liability and/or criminal sanctions
Thailand	Comprehensive	No	Personal Data Protection Committee	Personal liability and/or criminal sanctions
Vietnam	Information security law	Yes	Ministry of Information and Communications	None

Table of primary privacy regulation and regulator

Location	Legislation	Regulator
Australia	Privacy Act 1988 (Cth)	Office of the Australian Information Commissioner https://www.oaic.gov.au/
Brunei	Data Protection Policy 2014	Minister at the Prime Minister's Office http://www.pmo.gov.bn
Cambodia	The Constitution of the Kingdom of Cambodia	N/A
China	People's Republic of China Cybersecurity Law 2017	Cyberspace Administration of China http://www.cac.gov.cn./
Hong Kong	Personal Data (Privacy) Ordinance 1996	The Office of the Privacy Commissioner for Personal Data https://www.pcpd.org.hk/
India	Information Technology Act 2000	N/A
Indonesia	The 1945 Constitution of the Republic of Indonesia	Ministry of Communication and Information Technology https://www.kominfo.go.id/
Japan	Act on the Protection of Personal Information 2017	Personal Information Protection Commission https://www.ppc.go.jp/en/
Lao PDR	Law on Electronic Data Protection 2017	Ministry of Posts and Telecommunications https://www.mpt.gov.la/
Malaysia	Personal Data Protection Act 2010	Personal Data Protection Department http://www.pdp.gov.my Malaysian Communications and Multimedia Commission https://www.mcmc.gov.my/
Mongolia	Personal Secrecy (Privacy) Act 1995	N/A
Myanmar	Law Protecting the Privacy and Security of the Citizen 2017	Ministry of Home Affairs http://www.myanmarmoha.org/ Ministry of Communications and Information Technology http://www.mcit.gov.mm/
New Zealand	Privacy Act 1993	The Office of the Privacy Commission https://www.privacy.org.nz/

Papua New Guinea	Constitution of the Independent State of Papua New Guinea	N/A
The Philippines	Data Privacy Act of 2012	National Privacy Commission https://www.privacy.gov.ph/
Singapore	Personal Data Protection Act 2012	Personal Data Protection Commission https://www.pdpc.gov.sg/
South Korea	Personal Information Protection Act 2011	Personal Information Protection Commission http://www.pipc.go.kr/cmt/main/english.do
Sri Lanka	N/A	Information and Communication Technology Agency https://www.icta.lk/
Taiwan	Personal Information Protection Act 2010	Personal Data Protection Office
Thailand	Personal Data Protection Act	Personal Data Protection Committee
Vietnam	Law on Network Information Security	Ministry of Information and Communications https://english.mic.gov.vn/Pages/home.aspx

Acknowledgements

We would like to thank the following Deloitte professionals for their support and contribution to this publication:

Margaret Austen
Analyst
Australia

Paul Casey
Senior Analyst
Australia

Marie Chami
Manager
Australia

Erika Chin
Manager
Australia

Sung Kyo Cho
Director
South Korea

Nakul Chopra
Senior Manager
India

Karen Grieve
Director
Australia

Ho Kyoo Hahn
Senior Manager
South Korea

Div Jamdagni
Analyst
Australia

Kwon ho Ka
Manager
South Korea

Sebastian Le Cat
Senior Analyst
Australia

Eric Leo
Director
Australia

Richard Li
Analyst
Australia

Brad Lin
Director
Hong Kong

Max Lin
Director
Taiwan

Joanne Lu
Director
New Zealand

Toshiyuki Oba
Senior Manager
Japan

Pauline Pang
Senior Analyst
Australia

Herbert Rollom
Manager
The Philippines

Pedro Saa
Senior Analyst
Australia

Ilana Singer
Manager
Australia

Imogen Smith-Waters
Senior Analyst
Australia

James M Walton
Partner
Singapore

Jasmin Wong
Senior Analyst
Australia

Phoebe Wong
Manager
Hong Kong

Vincent Yin
Analyst
Australia

Sun Hee You
Director
South Korea

Maria Zotti
Analyst
Australia

Contacts

Manish Sehgal
Partner
Asia Pacific
+91 124 679 2723
masehgal@deloitte.com

David Batch
Partner
Australia
+ 61 2 8260 4122
dbatch@deloitte.com.au

Frank Xiao
Partner
China and Hong Kong
+86 108 512 5858
franxiao@deloitte.com.cn

Manish Sehgal
Partner
India
+91 124 679 2723
masehgal@deloitte.com

Haruhito Kitano
Partner
Japan
+81 80 3591 6426
haruhito.kitano@tohmatsu.co.jp

Anu Nayar
Partner
New Zealand
+64 2 1207 9573
anayar@deloitte.co.nz

Anna Marie Pabellon
Partner
Southeast Asia
+63 2 581 9038
apabellon@deloitte.com

Young Soo Seo
Partner
South Korea
+82 2 6676 1929
youngseo@deloitte.com

Chia-Han Wu
Partner
Taiwan
+886 2 4051 6888
chiahwu@deloitte.com.tw

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2019 Deloitte Asia Pacific Services Limited