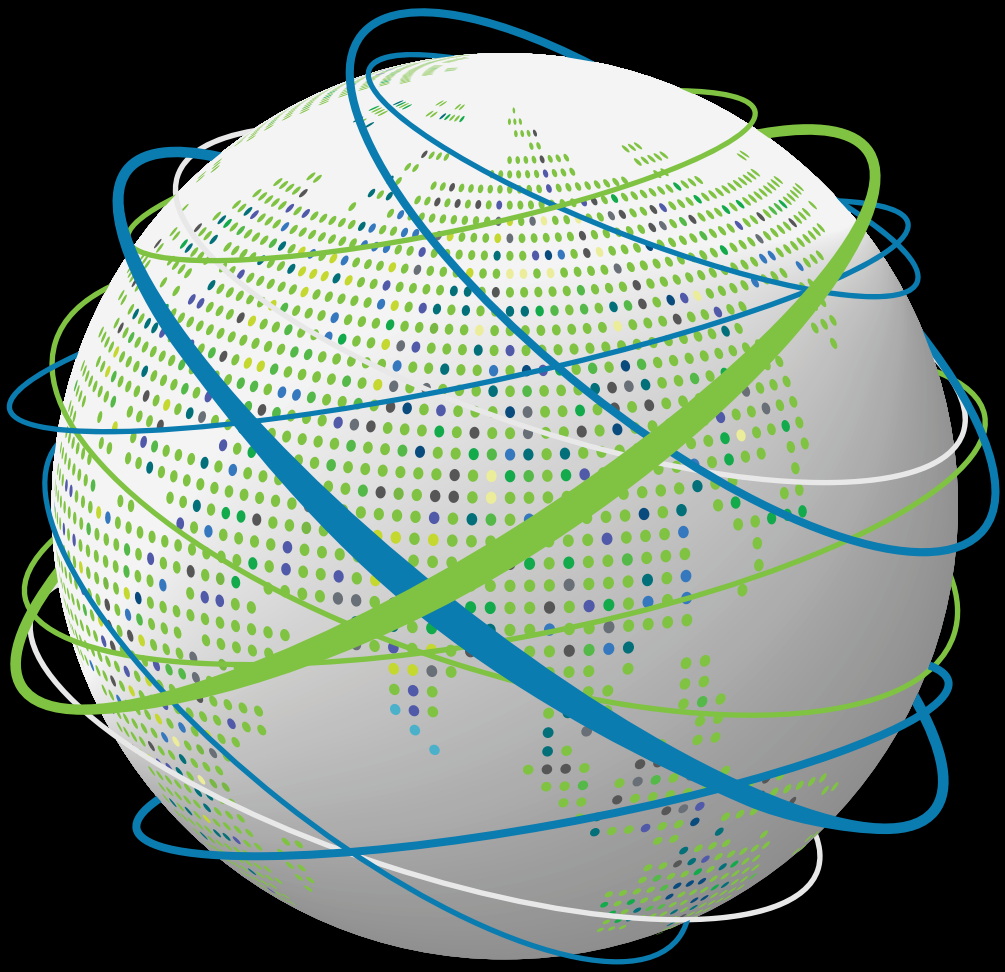
Deloitte.



The Asia Pacific Privacy Guide 2020-2021

Stronger together

December 2020

Contents

Introduction

For businesses operating in the Asia Pacific region, it is important to know how to navigate a diverse set of privacy and data protection regulatory and legislative requirements. These very distinct requirements span a wide variety of regimes – from Cambodia, Bangladesh and Myanmar, which all currently lack formal data protection and privacy laws, to the more comprehensive data protection and privacy regimes in Japan, South Korea and Australia.

The requirements continue to develop, with India and Indonesia both likely to introduce new privacy legislation shortly, and Singapore, South Korea, Japan and New Zealand all in the process of amending their existing privacy legislation frameworks.

Then there was COVID-19, which has further complicated the privacy landscape. COVID-19 has triggered a variety of technological measures to track and trace individuals with symptoms of the virus. Such measures inevitably require privacy and data protection, as contact tracing necessitates potentially processing an individual's whereabouts and personal health information.

Globalisation and COVID - the regulatory accelerators
Informed by the European Union (EU) General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), a number of regimes across the region have either amended, released, or reviewed their data privacy regulations and frameworks over the past year in order to encourage global alliances and investment. However, then COVID-19 created its own challenging and immediate pandemic requirements.

For instance, to remove the blanket 'data localisation' requirements, India amended its 2018 draft privacy bill, known as the Personal Data Protection Bill. Under the 2019 draft law, the personal data of a 'Data Principal' may be freely transferred, while the transfer of sensitive personal data attracts certain restrictions. However, then critical data, (yet to be defined in the bill), can only be stored in India and transfer is restricted.

Japan, as a corollary to its favourable EU adequacy decision, amended its privacy act for individual rights, including the broadening of an individual's rights to erasure and restriction of processing. And Singapore and New Zealand introduced mandatory breach reporting requirements in a 2020 amendment to their privacy regulations and legislations.

Introducing this guide

Given all this activity in the region, we felt it important to update this Deloitte Asia Pacific Privacy Guide, now in its third edition (2020-2021), and identify specific privacy and data protection laws, regulations and amendments in each of the Asia Pacific locations we cover. We also link to the specific official resource where available to ensure you have the most up to date information.

Increasing globalisation, coupled this year with the impact of the pandemic, has meant a significant focus on existing data privacy rules across the Asia Pacific region and a general interest in harmonisation. To this end we call out six key privacy trends across the region. And as a useful reference tool, we also compile a table of the technological measures used by each regime to trace and track individuals for COVID-19.

The guide is aimed at assisting business, risk, and compliance specialists with a general understanding of the nuances of the privacy requirements across Asia Pacific. Note, it is not intended to be a complete legal reference and should not be relied upon for that purpose. We trust you will find it useful. At the same time, we encourage you to consult a privacy specialist for any detailed specifics. All information presented in this guide is accurate and up to date as of November 2020.

Manish Sehgal
Asia Pacific Cyber Data & Privacy leader
Deloitte

James Nunn-Price
Asia Pacific Cyber leader
Deloitte

Emerging trends across the region

Given increasing global cyber threats, essential regional and global changes to data privacy and data protection frameworks, the ongoing adoption of the EU's GDPR and the need to combat the COVID-19 pandemic, there has been a progressive effort in the Asia Pacific region to harmonise. This includes introducing mandatory breach reporting requirements and cross-border data transfer requirements.

We note and highlight six key trends below.

Trend 1:
Privacy considerations viz COVID-19's tracking and tracing technology applications (apps)

As the COVID-19 scourge scars the globe, most Asia Pacific regimes have deployed various technologies to track and trace symptomatic and COVID-19 positive individuals. In general Bluetooth® or GPS-based contact tracing applications are used as location monitors and lockdown enforcement supports.

The technologies employed to monitor lockdown go a level beyond just tracing patients. They include facial recognition software systems for home-quarantined individuals, real-time geotagging-enabled selfie-based hourly check-ins, and electronic fence smart monitoring using a mobile phone's location data. These measures have focused regulators' and legislators' attention on data privacy considerations, highlighting the demarcation between civil liberties or privacy rights and the public interest, which is healthcare, life and livelihoods.

As remote working in lockdown has also had to be introduced where possible, organisations have accelerated their digital transformation strategies to ensure their business' continuity with 'work from home' measures. To manage data security and, where necessary, productivity, within the parameters of applicable employment and surveillance laws, many organisations have been exploring data protection and privacy controls.

These measures can include software that logs keyboard strokes or mouse clicks, screen freezes or auto-logouts based on webcam feed and activation. In this way employers can determine if the employee is using their monitor. Understandably, such measures attract privacy consideration dialogue. This has triggered the Office of Australian Information Commissioner to issue guidelines on assessing privacy risks in changed working environments[1] and China to issue a 'Cybersecurity Standards Practice Guide for Protecting Remote Working Security'.

How can you prepare?

- Consider whether the application is mandatory or voluntary
- Develop guidelines and best practices for employees to use the application
- Consider how employees may be affected by the COVID-19 monitoring measures and be transparent about what information is collected and why.

[1] https://www.oaic.gov.au/privacy/guidance-and-advice/assessing-privacy-risks-in-changed-working-environments-privacy-impact-assessments/

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

According to Article 45 of the GDPR, obtaining a favourable 'adequacy decision' means fewer restrictions on cross-border transfers of personal data for businesses between a designated 'adequate' regime and the EU. While New Zealand and Japan are the only nations within the Asia Pacific region with an adequacy decision from the European Commission, other regimes are either introducing, revising or strengthening their privacy regulations and legislations in order to obtain a favourable adequacy decision. South Korea for example has revised its regulations and legislation to be able to apply for an adequacy decision.[2]

How can you prepare?

- Ensure that transfers and disclosures of personal data are governed by written contracts and accompanying security controls to protect them during and after such disclosures
- Explore data transfer channels like Binding Corporate Rules and Data Protection Agreements.

Trend 3:
Mandatory data breach notification regulation and legislation

The shift to digitisation and online processing places businesses at significant risk of cyber-attack and data breaches. This has motivated governments across the Asia Pacific region to introduce breach reporting requirements that hold organisations to account for any data breaches, whether due to a third party, or services and online platforms exposed to social media or shared services. In 2020, Singapore, New Zealand and Malaysia all proposed introducing mandatory breach notification schemes to their respective legislative frameworks.

How can you prepare?

- Create an enterprise-wide process to manage privacy related complaints notified by third parties, customers and employees
- Consider developing a complaints process where a breach complaint can be lodged and reviewed, classified if so determined, and then investigated, tracked and capable of notifying relevant parties.

Trend 4:
Increased consumer and organisational awareness due to data breaches

Due to the recent proliferation of high-profile data breaches, consumers are increasingly aware of privacy regulations and legislation, and of their data privacy rights. As they become more conscious about the types of data they share, with whom, and where, they are compelling organisations to lift their privacy and cybersecurity postures. This has meant organisations are seeking to improve consumer trust and are establishing and implementing comprehensive privacy programmes.

How can you prepare?

- Consider developing a transparent and easy to comprehend privacy policy for individuals that details the legitimate purpose for processing personal information, the grounds for transferring any personal information and their individual rights, including the channels for exercising such rights.
- Create a consent management process that gives individuals control of how their personal information is processed beyond the original purpose of collection, consent withdrawal and transfers.

[2] https://www.dataguidance.com/opinion/south-korea-long-road-adequacy

Trend 5:
Interplay of cybersecurity and privacy regulation and legislation

In 2020, Cambodia, Sri Lanka and China, proposed or introduced cybersecurity regulations and legislation to curb unauthorised access to personal information, the spread of malicious software and digital hacking of computer devices and/or networks. While cybersecurity regulations and legislation govern and regulate the confidentiality, integrity and availability of personal information, they are supplemented by enforcing privacy regulations and legislation. This linkage serves as an added advantage as it enables the development of an enterprise wide compliance framework which factors in both organisational (policies and procedures) and technical (encryption and password protection) measures to facilitate privacy and protection of personal information.

How can you prepare?

- Create a policy that details appropriate cybersecurity measures and controls to adequately protect personal information, prevent breaches and personal information loss
- Enable protocols and controls to transmit personal information securely internally and externally. For example, introduce end-to-end encryption, centralised, protected and access-controlled repositories and multi-factor authentication for access to personal information.

Trend 6:
Facial recognition systems at airports

Some regimes in the Asia Pacific region are either implementing or conducting facial recognition system trials at airports when boarding the flight or at immigration control. India for instance, launched paperless biometric technology at Bengaluru and New Delhi airports[3] to identify passengers facially. This removed the need for boarding passes, passports or other identity documents. In Japan[4], six major airports are currently deploying an electronic customs procedure system that uses facial recognition technology. While there is a clear case for greater security and efficiency when it comes to boarding procedures, it is important to balance efficiency with guidance and appropriate regulations to protect privacy rights, ensure accuracy and secure personal data.

[3] https://scroll.in/article/929851/facial-recognition-as-airports-in-india-start-using-the-technology-how-will-it-be-regulated
[4] https://www.futuretravelexperience.com/2019/07/six-major-airports-in-japan-set-to-adopt-facial-recognition/

COVID-19 technology and privacy

The COVID-19 pandemic created new security and privacy challenges due to the various contact tracing technologies deployed across the Asia Pacific region. This compelled industry, public organisations and governments to explore ways to maintain the balance between public health and personal privacy. We compile the Asia Pacific technological interventions at the time of writing in the table below along with related considerations for personal and health data.

Location	Name of Contact tracing technology	Overview of the technology
Australia	COVIDSafe	The Australian government launched its contact tracing application *COVIDSafe* to help find people who have been in close contact with positive cases. The app collects personal information including name, mobile number, post code and age range. It also creates a unique encrypted reference code for the user. The *COVIDSafe* app recognises other devices with the *COVIDSafe* app installed and with Bluetooth® enabled. When the app recognises another user, it notes the date, time, proximity, duration of the contact and the other user's reference code. It does not send pairing requests. The information is stored on the device and is deleted on a 21-day rolling cycle. The encrypted information is only uploaded to a secure government server when someone is diagnosed with COVID-19 and the user provides permission for such upload.[5] It also provides information on the total confirmed cases by state and territory, it offers help topics, provides information in nine other languages, explains Bluetooth® settings, advises how to remove the app and how to upload your information if you have tested positive, carries the relevant government standards, and details how the app works.
Bangladesh	Corona Identifier	The government of Bangladesh introduced the *Corona Identifier* contact-tracing application to combat the outbreak of COVID-19. Launched by the Post and Telecom Ministry, the application was jointly developed by state-run mobile operator Teletalk and Radisson Digital Technologies Limited.[6] The app shares both location monitoring and sensitive health information and so will require an individual's privacy rights to be balanced against public health concerns.

[5] https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
[6] https://www.dhakatribune.com/bangladesh/2020/04/05/corona-identifier-app-launched-in-bangladesh

Location	Name of Contact tracing technology	Overview of the technology
China	Health Code	The Chinese government monitored the COVID-19 outbreak with an app service called *Health Code*. The app told citizens whether to carry on as usual or report to a medical facility to be quarantined. Integrated into the Alipay and WeChat apps, *Health Code* lets citizens check if they had been in close contact with anyone diagnosed with COVID-19. It provided colour-coded designations based on the user's health status and travel history, along with a QR code that could be scanned by authorities.[7]
Hong Kong	StayHomeSafe	The government of the Hong Kong Special Administrative Region launched its *StayHomeSafe* mobile app to trace the contacts of people subject to compulsory quarantine. Emphasising the need to create a balance between COVID-19 patients' privacy rights and public health, the Privacy Commissioner for Personal Data relied on the Data Protection Principle 1 of the PDPO to ensure that both the means of collecting personal data was lawful and fair, and that the data collected was to protect the public from any serious threats to public health.
India	Aarogya Setu	The Ministry of Electronics and Information Technology launched its contact-tracing application, *Aarogya Setu*,[8] using the concept of 'privacy by design' in its development process. The privacy policy was updated post launch to include details of purpose, collection limitation, retention periods, data use and third-party disclosure, storage location and consent. The updated privacy policy reiterated that personal information would not be shared with any third party, unless to carry out necessary medical and administrative interventions. It was also specific about the purpose and use of any data collected, including: • minimising data collection and linking individual information to a unique digital ID • limiting data use to anonymised and aggregated data sets for generating reports, heat maps, and communication on probability of infection • calculating a user's probability to develop the infection using Bluetooth® range and GPS location • storing location data securely on a mobile device • obtaining consent before uploading risk assessment test results to the government server.

[7] https://www.loc.gov/law/foreign-news/article/china-citizens-must-obtain-green-health-code-to-board-flights-returning-to-china/
[8] https://meity.gov.in/content/aarogya-setu-data-access-and-knowledge-sharing-protocol-2020

Location	Name of Contact tracing technology	Overview of the technology
Indonesia	TraceTogether	The Indonesian Ministry of Communication and Informatics (KOMINFO) issued Decree No. 159 of 2020 concerning COVID-19 Handling Efforts through Post and Information Sector, to cover implementing tracing, tracking, and fencing mechanisms through mobile applications and call phone messaging. The mechanism entails the collection, processing, analysis and dissemination of data to produce objective, measurable and comparable information for a particular time and place to assist in identifying COVID-19 positive individuals. The *TraceTogether* mobile app was developed collaboratively by the Ministry of Communication and Informatics (KOMINFO) and Indonesia's main telecommunications operators.[9] For up to 14 days the app collects the mobile phone location data of the infected person. It matches that data with the telecommunication companies' location data, so it can pinpoint and warn individuals who were in the patient's vicinity.[9]
Japan	COCOA	The Japanese government introduced *COCOA*,[10] a smartphone application that uses Bluetooth® signals to inform individuals if they had close contact with someone infected with COVID-19.[11] The app highlighted privacy violation concerns and triggered Japan's Personal Information Protection Commission to release guidelines on how best to secure and use personal information collected using *COCOA*.[12]
Lao	LaoKYC	The Lao Ministry of Post and Telecommunications launched a website and mobile application to help contain the spread of COVID-19. The app, *LaoKYC*, monitored the activities and locations of registered individuals and informed them if they had been in close proximity with an infected individual.[13]
Mongolia	Name unavailable	Law enforcement bodies in Mongolia used a mobile surveillance application installed on quarantined patients' mobiles to track their whereabouts and prevent community transmission of the disease. Identified individuals were required to have the app and forbidden to turn off their phones. This was to ensure their movements could be monitored at all times.[14] This surveillance application does challenge privacy concerns as it does not factor in choice, transparency or consent when collecting location and health related sensitive data.

[9] https://privacyinternational.org/examples/3565/indonesian-tracetogether-app-uses-location-data-contact-tracing
[10] https://www3.nhk.or.jp/news/html/20200619/k10012476441000.html
[11] https://english.kyodonews.net/news/2020/06/39a7184b5d65-japan-govt-offers-free-coronavirus-contact-tracing-app.html
[12] https://www.ppc.go.jp/en/legal/covid-19_2en/
[13] https://www.mpt.gov.la/index.php?r=site/detail&id=566
[14] https://news.mn/en/791435/

Location	Name of Contact tracing technology	Overview of the technology
Malaysia	Name unavailable	The Personal Data Protection Commission released its COVID-19 advisory guidelines on 29 May 2020. They cover the collection and handling of personal data by businesses that are allowed to operate under the 'Conditional Movement Control Order' during the outbreak of COVID-19. The guidelines specify that only names, contact numbers, dates and the times of entry to a premises can be collected. Collection requires providing an explicit notice to detail its purpose. The guidelines also state that the personal data collected must be permanently deleted within six months after the Conditional Movement Control Order is terminated.[15]
New Zealand	NZ COVID	The New Zealand Ministry of Health released its *NZ COVID* contact tracer application to manage the COVID-19 pandemic outbreak.[16] The information shared by the app was securely stored on the user's phone and automatically deleted after 31 days. The sharing by an individual of any information collected with contact tracers for public health purposes was voluntary.
Philippines	DataCollect	The Filipino Department of Health launched its *DataCollect* application to track COVID-19 positive individuals.[17] The app provides a snapshot of the Department's pandemic capability including information on testing, health facilities and personal protective equipment availability. The National Privacy Commission promotes the application as a way of helping health authorities contain the pandemic and issued guidelines on the collection, use and disclosure of personal and sensitive information of patients. The Commission specified only collecting and disclosing essential information to combat COVID-19 to relevant authorities.
Singapore	TraceTogether and SafeEntry	The Singapore government launched its *TraceTogether* application that registers Bluetooth® signals with nearby phones running the same app. Although GPS data is not collected, identity data, including the mobile number and a random anonymised user ID, are collected. The data is stored on the user's device and the application does not enable third-party tracking of its data. Tracking is only enabled if the individual tests positive for COVID-19. The application also allows users to withdraw consent for processing of their data. In addition, on 9 May 2020, Singapore's Ministry of Health and Smart Nation and Digital Government Office released its digital check-in application, *SafeEntry*. This app captures an individual's personal data

[15] https://www.mdbc.com.my/mco-updates/
[16] https://www.health.govt.nz/news-media/media-releases/nz-covid- tracer-app-released-support-contact-tracing
[17] https://www.doh.gov.ph/doh-press-release/DOH-LAUNCHES-NEW-COVID-19-TRACKER-AND-DOH-DATACOLLECT-APP

Location	Name of Contact tracing technology	Overview of the technology
		either by scanning their National Registration Identity Card, or on entry to a business premises using a QR code on their mobile device to record arrival and departure times. Data collected by individual businesses via this application is sent directly to the government. Singapore's Personal Data Protection Commission released advisories on the collection of personal data and use of this *SafeEntry* application.[18]
South Korea	Corona 100m (Co100)	The *Corona 100m (Co100)* app was launched in South Korea in February 2020 to alert users when they were within 100 metres of a location visited by an infected person.[19] The application therefore warns users to avoid potentially dangerous locations without needing to check the travel histories of the COVID-19 positive. The application does however raise questions on how to reconcile public health protection and privacy, as the unauthorised disclosure of a user's sensitive health and location data is at stake.
Sri Lanka	COVID Shield	Sri Lanka leveraged its already developed capabilities of surveillance systems based on its Open Source DHIS2 platform. It also launched a *COVID Shield* mobile application[20] for users to track their health and to provide them with support during self-isolation and quarantine. The app enables users to regularly assess their lung health and identify any potential deterioration early on through their smart phone's recording features. The recorder gathers and analyses additional data when the user performs simple breathing tests. Data related to the health of the user and location is subject to a centrally managed secure database to ensure privacy and confidentiality.
Taiwan	Name unavailable	The National Communications Commission launched an 'electronic fence smart monitoring system'. In this system, anyone required to undergo home quarantine has their location monitored via cellular signals from their mobile phone. Venturing too far from home triggers an alert to local authorities. Subsequently, calls and messages are sent to the individual to ascertain their whereabouts. Anyone caught breaching quarantine can be fined up to NT$1 million.[21] On 28 May 2020, the Central Epidemic Command Center (CECC) announced additional contact guidelines applicable to all industries.

[18] https://www.pdpc.gov.sg/Help-and-Resources/2020/03/Advisory-on-Collection-of-Personal-Data-for-COVID-19-Contact-Tracing
[19] https://qz.com/1810651/south-koreans-are-using-smartphone-apps-to-avoid-coronavirus/
[20] https://echalliance.com/commonwealth-centre-for-digital-health-cwcdh-response-to-covid-19-pandemic-covid-shield/
[21] https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK

Location	Name of Contact tracing technology	Overview of the technology
		They emphasised personal data protection and extended venue proprietors' obligations to collect customer personal data and the requirement to designate a person to be in charge of keeping and maintaining records of personal data processing activities. Personal data can be retained for no longer than 28 days, after which it should be deleted. It can only be used in conjunction with the health authority's epidemic investigation. Any other use of the data is not permitted. Personal data can also be collected electronically or in writing, and anyone found in violation of these requirements can be fined up to NT$2 million per Taiwan's Personal Data Protection Act (PDPA).[22]
Thailand	Thai Chana	Thailand's Center for COVID-19 Situation Administration (CCSA) launched its contact tracing application *Thai Chana* (Thai Victory) for all businesses. Businesses can register online for the app and for a QR code to display in their premises for customers to scan when entering and exiting. If a customer had been to a venue visited by a COVID-19 positive individual a text message is sent to the customer indicating they may need to be tested. Privacy guidelines were not deemed necessary in this case because section 26 of the Personal Data Protection Act permits processing health-related data when undertaking a preventive measure to protect the health of a person.
Vietnam	Bluezone	Technology firm Bkav and the Ministry of Information and Communications joined forces to release the COVID-19 contact-tracing application, *Bluezone*. Using Bluetooth signals, it links smartphones within two metres of each other that have downloaded the app. It notifies users if they have been in the proximity of a COVID-19 positive patient in the past 14 days.[23] The application collects a user's identity, health and location details, requiring the user's permission to record location and media e.g. photographs, due to privacy concerns.

[22] https://www.cdc.gov.tw/En/Bulletin/Detail/pevkg6JalT40I4uB6wAWcg?typeid=158
[23] http://hanoitimes.vn/vietnamese-people-asked-to-install-app-for-covid-19-contact-tracing-313703.html

Privacy guides for Asia Pacific

Updates for privacy and data protection regulation, related amendments and key trends for the Asia Pacific region have been detailed in the following sections.


Australia


Bangladesh


Brunei Darussalam


Cambodia


China


Hong Kong


India


Indonesia


Japan


Lao People's Democratic Republic


Malaysia


Mongolia


Myanmar


New Zealand


Papua New Guinea


The Philippines


Singapore


South Korea


Sri Lanka


Taiwan


Thailand


Vietnam

How to use this guide

Each legislative profile covers the following:

Primary legislation	The key privacy law(s) and/or regulation(s) for that location
Key considerations	Highlights of the latest trends in the realm of privacy, data protection and cybersecurity
Definition of personal information	How the primary legislation defines personal information and sensitive personal information
Collection and notice	The requirements around the purposes for which personal information may be collected and the obligations that may exist around providing notice to individuals before or when collecting their personal information
Use and disclosure	The requirements around how personal information may be used and disclosed to others
Data retention and destruction	The requirement around retaining personal information as per a legitimate purpose. The requirement additionally pertains to personal information retention periods and destruction mechanisms.
Individual rights	The rights individuals are granted over their personal information, such as the rights of access, correction and objection to processing
Security	The requirements around the protection of personal information, such as protection from misuse, interference, loss, unauthorised access, modification and disclosure
Data breach notification	The requirements that may exist around notifying the relevant authority and/or any affected individuals in the event of a data breach
Cross-border data transfer	The requirements covering the transfer of personal information outside of territorial boundaries
Governance	The requirements, if any, pertaining to the appointment and functions of a data protection/privacy officer (DPO)
Regulators and regulatory landscape	The key privacy regulator, its organisational structure, responsibilities and functions with respect to privacy and data protection
Cases	A snapshot of select relevant and recent cases relating to breaches of privacy law and/or regulations
Penalties	The penalties and sanctions that may be levied in the event of non-compliance with, or breach of, privacy law provisions
Relevant laws, directives and terminology reference	A summary table of the laws and regulatory directives around privacy and data protection, along with definitions for key terminology

These profiles are then supplemented with:

- **a comparison matrix:** a visual comparison of selected privacy elements covered in the Asia Pacific region at the time of writing
- **a regulatory landscape table:** The privacy regulatory landscape across Asia Pacific at a glance
- **a table of primary privacy regulations and regulators:** overview of the name of the primary privacy legislation along with the names and web addresses of the regulators covered in this guide.

Australia

Privacy in Australia is primarily regulated through a comprehensive federal law, the Commonwealth Privacy Act 1988, which is centred on the Australian Privacy Principles. The Privacy Act applies to all federal government agencies and private sector entities with an annual turnover of at least A$3 million. Most states in Australia, other than Western Australia and South Australia, have their own privacy laws that are applicable to state government agencies. Personal information is also regulated under other legislation, including the Workplace Surveillance and Health Records Acts, which are governed at the State level.

Primary legislation: Privacy Act 1988 (Cth)

Key considerations:

Digital platforms enquiry:[24] On 26 July 2019, the Australian Competition & Consumer Commission (ACCC), the Commonwealth authority responsible for enforcing competition and consumer-related legislation, released its final report of an inquiry focussed on digital platforms. The inquiry covered online search engines, social media platforms and other digital content aggregation platforms. It was initiated due to concerns around inadequate market and bargaining power in the competition space and concerns pertaining to trust, welfare and protection in the consumer area. The report addressed these concerns and recommended major reforms of the Privacy Act to help ensure that privacy settings empower consumers, protect their personal information and best serve the Australian economy.

Privacy act law reforms:[25] Following this Digital Platforms Inquiry report, the federal government announced a broad review of the existing Privacy Act with advice provided directly by the Office of the Australian Information Commissioner (OAIC). It is expected to be finalised in 2021. Areas for review include the definition of personal information, notice and consent requirements, penalty increases, and the right to request erasure of personal information. The report also states that the government intends to introduce a direct right of action for individuals to seek compensation for interference with their privacy.

[24] https://www.mondaq.com/australia/privacy-protection/840242/new-penalties-recommended-for-privacy-infringements
[25] https://treasury.gov.au/sites/default/files/2019-12/Government-Response-p2019-41708.pdf

Privacy code for digital platforms: The OAIC is working with the Australian government and other stakeholders to develop a binding code for digital platforms that trade in personal information. The code is expected to:

- require platforms to cease use and disclosure of personal information on request
- require specific consent for the handling of personal information
- provide stronger protections for children and other vulnerable Australians.

Open banking and the Consumer Data Right (CDR):[26] The CDR provides customers with greater access to and control over their data, enabling them to compare and switch between products and services to encourage competition in the market and provide better prices and innovative products for customers. It was introduced 6 February 2020, following announcement in November 2017. The ACCC is the lead regulator for the CDR and will operate in tandem with the OAIC and Data Standards Body to develop and implement the right. The CDR will be applied in phases, starting with the banking sector, followed by energy and utilities, and finally telecommunications. In February, the OAIC developed guidelines about privacy obligations and how to safeguard privacy for consumers as part of the scheme. To help inform businesses that operate under the CDR, the OAIC was supported by consultations with industry, the ACCC, and other stakeholders.

Data breach notifications:[27] Mandatory data breach notifications have been in place since February 2018. The OAIC reported a 19% increase in the number of notified data breaches between July and December 2019, with 64% of the total (537) attributable to malicious or criminal attacks and 32% to human error. Health and finance are the two sectors that suffered the most data breaches.

Australian government agencies privacy code (the Code): TThe Code sets out specific requirements for Australian government agencies to implement privacy governance and has been in place since July 2018. It requires agencies to have a privacy management plan, appoint a privacy officer and privacy champions, and undertake Privacy Impact Assessments for all high-risk projects.

Online privacy: There are no laws or regulations in Australia that specifically relate to online privacy. If cookies or other similar technologies, such as applications, collect personal information, the organisation is required to comply with the Privacy Act for collection, use, disclosure and storage. Detailed guidelines are provided by the Privacy Commissioner.

[26] https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/commencement-of-cdr-rule
[27] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/Notifiable-Data-Breaches-Report-July-December-2019.pdf

Definition of personal information

The Australian 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, or 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.

Collection and notice

Personal information, other than sensitive information, should only be collected if it is 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, deidentified 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.

Use and disclosure

Personal information can only be used for the original purpose for which it was collected unless certain conditions are met. These include if an individual has consented 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 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 for which it was collected. If no longer required for a particular purpose, the information should be securely destroyed or deidentified.

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. Organisations must respond within 30 days or inform the individual if 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.

Data breach notification

On 22 February 2018, the mandatory data breach notification regime commenced in Australia. The Commissioner and data subjects must be notified of 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.
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.

Data transfer

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

Governance

Although organisations are not required to appoint a data protection officer, the Commissioner provides guidance for organisations to appoint such an officer 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 include:

- conducting investigations into activities which may breach the Privacy Act
- reviewing decisions made under the Freedom of Information Act, 1982
- managing complaints about the handling of personal information
- providing privacy advice to the public, government agencies and businesses.

Cases

- **2020** – a telecommunications provider mistakenly published information relating to 50,000 customers in the White Pages. The data breach was discovered by the company during a routine audit. The types of information involved included names, home addresses and phone numbers.[28]
- **2020**– a logistics provider suffered a ransomware attack (Nefilim) where information was stolen directly from a corporate server and was published on both the dark web and a publicly accessible website hosted by the threat actor. The company refused to pay a ransom at the threat actor's request and as a result, the actor has claimed its intention to release 200GB of information in a series of leaks. The type of information accessed and stolen relates to past and present employees and commercial agreements.[29]
- **2020**– an educational institution reported in March that it suffered a data breach that exposed personal information relating to more than 50,000 staff and students held on IT systems. The data breach occurred between September and December 2018 and was reported in October 2019 after an investigation by the Victoria Police. The breach affected 90,000 students, staff and suppliers, and included a combination of email addresses, usernames, passwords, financial and health information.[30]

Penalties

According to the Commonwealth Privacy Act, 1988:

- the Commissioner will investigate an act or practice that may interfere with the privacy of an individual, as well as any complaint about the act or practice 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 that is not settled, the results of that investigation must be made publicly available by publishing the investigation report on the OAIC website
- after investigating a complaint, the Commissioner may dismiss the complaint, or substantiate the complaint and declare that the organisation rectify its conduct or compensate for any loss or damage suffered by the individual.
- the Commissioner may request the courts impose fines of up to A$420,000 for an individual and A$2.1 million for corporations for serious or repeated privacy breaches.

[28] https://m.dailyhunt.in/news/nepal/english/telangana+today+english-epaper-teltdyen/optus+sued+after+50k+aussie+s+details+leaked+to+white+pages-newsid-n180970184
[29] Information coming directly from Deloitte CTI threat notification: Nefilim Ransomware-as-a-Service (Raas) operators leak stolen data obtained in Toll Group ransomware attack.
[30] https://portswigger.net/daily-swig/australia-data-breach-90-000-staff-students-suppliers-impacted-at-melbourne-polytechnic#:~:text=Compromised%20files,information%20accessed%20during%20the%20breach.

Relevant laws, directives and terminology reference

Law, regulation, guideline or standard	Industry	Regulator	Applicability
Competition and Consumer (Consumer Data Right) Rules 2020	All	The Australian Competition and Consumer Commission	CDR participant
The Privacy Safeguard Guidelines	All *Only applies to the banking sector currently; however, will apply to energy and telecommunications in the near future as the CDR will be rolled out in phases	Office of the Australian Information Commissioner (OAIC)	CDR participants
Freedom of Information Act 1982	Government	Office of the Australian Information Commissioner	Government
My Health Records Act 2012	Health sector	Office of the Australian Information Commissioner	Health care providers
Privacy Credit (Reporting Code) 2014	Financial services	Office of the Australian Information Commissioner	Credit Providers and Credit Reporting Bodies
Prudential Practice Guide CPG 235 Managing Data Risk	Financial services	Australian Prudential Regulation Authority	Financial services
Prudential Standard CPS 234 Information Security	Financial services	Australian Prudential Regulation Authority	Financial services
SPAM Act 2003 (Cth)	All	Australian Communications and Media Authority	Comprehensive
Telecommunications Act 1977	Telecommunications	Office of the Australian Information Commissioner	Telecommunications carriers and carriage service providers
Telecommunications (Interception and Access) Act 1979	Telecommunications	Office of the Australian Information Commissioner	Telecommunications carriers and carriage service providers
Telecommunications and Other Amendments (Assistance and Access) Act 2018 (Cth)	Telecommunications	Office of the Australian Information Commissioner (OAIC)	Telecommunications carriers and carriage service providers

Terminology	Definition
Agency	refers to Australian government (and Norfolk Island government) agencies but does not include state and territory agencies.
APP entity	is an agency or organisation required to comply with the Australian Privacy Act, 1988.
CDR participant	is a data holder or an accredited data recipient of the CDR.
COVID-19	Coronavirus Disease 2019
Organisation	an 'organisation' is defined as: • an individual (including a sole trader) • a body corporate • a partnership • any other unincorporated association • a trust unless it is a small business operator, registered political party, state or territory authority or a prescribed instrumentality of a state.

Bangladesh

Bangladesh does not have a comprehensive legislative regime or regulatory body responsible for privacy. The basic framework for data protection and privacy is laid out under the Constitution of Bangladesh, along with the Information Communication Technology Act 2006[31] and the Digital Security Act 2018.[32]

Primary legislation: Digital Security Act, 2018 (DSA)[33]

Key considerations:

e-Government master plan for Digital Bangladesh: The Bangladesh government is working to achieve the Digital Bangladesh Vision 2021 by establishing the Seventh Five-Year Plan (2016–2020) and the National ICT Policy 2015. The Bangladesh government recognises how critical information and communication technology is to the country's growth potential and is making significant efforts to improve its budget execution and administrative efficiency through e-Government.[34]

Definition of personal information

Personal information is not defined in the DSA. However, the DSA defines **'Identity information'** as any external, biological or physical information or any other information, which singularly or jointly can identify a person or a system, but is not limited to name, address, date of birth, fingerprint, passport number and/or iris image.

Data retention and destruction[35]

The Director General of the Digital Security Agency may, on its own accord, or on an application made by an investigation officer including the police, order an organisation to mandatorily preserve and retain identity information stored on a computer device for 90 days from the date of the order being issued by the Director General. The basis for the order being to protect the information from destruction and/or alteration due to an ongoing data breach investigation. The 90-day retention period may be extended for another 90 days on application to the Cyber Tribunal. However, the cumulative retention period cannot be more than 180 days from the date of the original order issued by the Director General.

[31] https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf
[32] https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf
[33] https://www.dpp.gov.bd/bgpress/bangla/index.php/document/extraordinary_gazettes_monthly/2018-10-02
[34] http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/ecbb5603_1eac_4bf0_99fe_628e9980c279/e-Government%20Masterplan%20for%20Digital%20Bangladesh_V6.0%20(2).pdf
[35] Section 44 Digital Security Act, 2018

Data transfer

If anyone accesses a computer or digital system without authorisation from the computer's or digital system's owner, and alters the identity information stored on the system, or transfers identity information belonging to a government, semi-government, autonomous or statutory organisation or any financial or commercial organisation, that activity will be considered an offence under the DSA.[36]

Regulators and regulatory landscape

The DSA has the authority to:

- remove or block (either by itself or through the Bangladesh Telecommunication Regulatory Commission) any data-information that threatens digital security, national solidarity, financial activities, security, defence, religious values, or public discipline, or that causes racism or hatred within Bangladesh
- create an emergency response team
- create a digital forensic lab.

The National Digital Security Council is the DSA's implementation agency. It provides directives on advancing an organisation's digital security infrastructure and develops inter-institutional policies to help ensure digital security.

Cases

- **In late 2018,** Pathao, a ride sharing service, was alleged to be improperly storing its users' identity information, including customer contact lists and SMS messages.[37]

Penalties[38]

The following penalties may be imposed by the DSA on identity, digital or electronic violations, infringements and omissions:

- Collecting, selling, preserving, supplying, or using identity information without the individual's explicit consent or authorisation is punishable by an imprisonment term of up to five years, or a penalty of up to ৳500,000 or both
- Any offence related to digital or electronic fraud subjects an individual to potential imprisonment for a term not exceeding five years, or a fine not exceeding ৳500,000 or both
- Identity fraud subjects the offending individual to potential imprisonment for a term not exceeding five years, or a fine not exceeding ৳500,000 or both
- If any person commits an offence related to the illegal transfer or saving of identity information, they may be sentenced to a term of imprisonment not exceeding five years, or a fine not exceeding ৳1,000,000 or both.

Note: Service providers will not be automatically held responsible under the DSA for merely providing a platform for accessing identity information, for example user generated content providers. However, the service provider will be required to furnish evidence regarding its lack of knowledge in relation to any offence or breach committed under the DSA in order to qualify for immunity from the provisions of the DSA.

[36] Section 33, DSA
[37] https://asiatimes.com/2018/11/dhaka-ride-sharing-app-accused-of-storing-users-phone-data/
[38] Chapter 6, DSA

Relevant laws, directives and terminology reference

Law/Decree	Industry	Responsible ministry	Applicability
ICT Guidelines 2015 for banking and non-banking financial institutions	Banking/finance	Ministry of Finance	Guidelines are applicable for banks and non-bank financial institutions, as well as their customers and stakeholders.
Constitution of Bangladesh	All	N/A	Subject to any reasonable restrictions imposed by law in the interests of the security of the state, public order, public morality or public health, Article 43 grants every citizen the right to the privacy of their correspondence and other means of communication.
Information Communication Technology Act, 2006	All	Ministry of Posts, Telecommunications and Information Technology	Applicable to person or body corporate that possesses, deals or handles any sensitive personal data or information.

Terminology	Definition
ICT	Information and Communications Technology
Service provider	• any person who through computer or digital process enables any user to communicate • any such person, entity or institution who or which preserves or processes data in favour of the service user.

Brunei Darussalam

Currently, the Data Protection Policy 2014[39] (DPP) acts as a guide for the protection of personal information within Brunei and applies to agencies. The DPP governs personal data maintained by all government ministries, departments, educational institutions, and statutory boards. However, the Prime Minister's office has acknowledged that an improved legal framework to protect personal data is required, especially given the implications arising from well-known global data breaches relating to social media platforms.[40]

In January 2019, the Minister of Transport and Info-communications confirmed his appointment as the minister responsible for the nation's cybersecurity which encompasses safeguarding personal data. The Brunei government's awareness of privacy and personal data protection and its move towards their regulation is in response to its cities holding more citizens' personal data.[41]

The Brunei government has also considered incorporating the privacy and data protection frameworks from neighbouring countries, including Malaysia and Singapore, into their design of laws and regulations. Progress of this anticipated legislative reform is yet to be formally announced.

Primary legislation: Data Protection Policy 2014 (for government data assets), Official Secrets Act (Chap. 153)

Key considerations:

Online verification portal development: In March 2018, the Prime Minister's office announced a plan to establish an online portal to limit the spread of fake news on social media, given reports of rising global and regional data misuse cases.

Definition of personal data[42]

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

When collecting data, the DPP mandates that agencies must do so fairly and lawfully, and specify the purpose for which the data is collected. The agency must notify the individual from whom the data is collected at or before the time the data is collected. In the event that this is not practicable, the individual must be notified as soon as reasonable after collection. The purpose for collection is to be specified in a manner that the individual can reasonably understand both why and how it will be used or disclosed. Its collection must be limited to the purpose specified by the agency.

[39] http://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf
[40] https://thescoop.co/2018/05/10/brunei-calls-legal-framework-protect-user-data-online/
[41] http://www.mtic.gov.bn/Lists/Speeches/NewDispItem.aspx?ID=142&ContentTypeId=0x01009E303218B4B09449AE6D253837EBB2FC
[42] http://www.information.gov.bn/PublishingImages/SitePages/New%20Media%20and%20IT%20Unit/Data%20Protection%20Policy%20V.2.2.pdf

Use and disclosure

Data shall not be used or disclosed to a third party for any purpose other than that for which it was collected, except where the consent of the individual has been obtained or where such disclosure is required by any applicable laws of Brunei Darussalam. Where it is impracticable to obtain an individual's consent, a legal guardian or power of attorney can provide consent on their behalf.

Consent is not required 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 the life, health or security of an individual exists
- the data is generally publicly available
- the use or disclosure is necessary to render a service the individual applies for
- disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance, and where the disclosure is for such purpose.

Data retention and destruction

Data shall be retained for only as long as necessary to fulfil the purpose for which it was collected unless required by the legislation to be retained for archival purposes. Agencies can develop internal policies, guidelines and procedures for retaining and destroying data. Reasonable care should be used when disposing or destroying personal data to prevent any unauthorised access to it.

Individual rights

Individuals have the right to:

- **be informed** of their rights prior to collection and the intended use of their personal data o
- **access** their personal data upon requesting details of its existence, use and disclosure
- **challenge** the accuracy and completeness of their data and have them amended as appropriate.
- **contest** the compliance levels of agencies (with respect to the DPP) and policies and procedures relating to the handling of personal data.

  Agencies can refuse an individual's request for access where providing access would be likely to reveal data about another individual. The reasons for denying access should be provided to the individual on receiving their request.

Security

To prevent any accidental or unlawful loss, unauthorised access, disclosure, use or modification, agencies should ensure all data is protected, regardless of how it is held. Agencies need to observe reasonable safeguards when disposing or destroying personal data to prevent any unauthorised parties gaining access to it. Methods to protect the data should include physical, organisational and/or technological measures. It is also important that employees are made aware of the significance of maintaining data confidentiality.

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 those of the DPP
- the individual has provided consent
- it is necessary for contractual or pre-contractual obligations
- reasonable steps have been taken to ensure the data will not be used, held or disclosed by the recipient inconsistent with the DPP's principles.

Governance

Agencies are responsible for all data, including personal data in its possession or custody. They must designate an officer or officers to ensure that the agency complies with its privacy policy. This officer, or other suitably nominated officer, will be responsible to implement the agency's policy, and monitor and manage it. This officer will also be responsible to carry out scheduled and unscheduled compliance checks to ensure adherence to the privacy policy.

The agency may also elect a team to support the designated officer in carrying out the responsibilities in relation to the privacy policy. The designated officer is obliged to report any non-compliance or data breaches at the agency to the administrator at all times. If required by the administrator, the designated officer shall assist in the investigation carried out by the administrator.

Regulators and regulatory landscape

Currently, there is no designated regulator for privacy. The Data Protection Policy 2014 is under the responsible authority and accountability of the minister at the Prime Minister's office and compliance with this policy in the Government shall be ensured by the e-Government National Centre known as the administrator.

The roles and responsibilities of the PMO's responsible authority and administrator include:

- administering and enforcing the DPP
- providing regular reports
- promoting awareness of data protection in the Government
- performing non-compliance or breach related investigations
- 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
- representing the Government internationally
- conducting research and promoting educational activity.

Penalties

If any user is found to have breached this policy, an investigation will be carried out by the administrator and they may be subject to government disciplinary procedures. If a criminal offence is considered to have been committed, further action may be taken to assist enforcement authorities prosecute the offender(s).

Exemptions

The following data processing activities are exempt from the requirements of the Data Protection Policy 2014:

- where required by any law or by the order of a court
- performed by an agency directly relating to a prospective, current or former employment relationship between the agency and the individual
- involving data related to any individual or organisation that is not held or stored electronically by the agency and is available to the public
- necessary for national and public security, national defence or internal security
- necessary to prevent, investigate, detect and prosecute criminal offences, breaches of ethics and rules for regulated professions the national economic or financial interest, including monetary, budgetary and taxation matters monitoring, inspection or regulatory functions, connected, even occasionally, with the exercise of official authority processing for research or statistical purposes, provided the results of the research or any resulting statistics involve techniques to prevent the identification of any specific individual by reasonably foreseeable means.

Cases

- **In 2018** Brunei reported a 39% rise in cyber-attacks, with malicious software accounting for the majority of 2,976 cases[43]
- **In 2019**, online store CafePress asked customers to choose new passwords as part of an updated 'password policy' after news broke about the store's website having been victim to a data breach. More than 23.2 million accounts were apparently exposed, including email addresses, names, physical addresses and phone numbers.[44]

Relevant laws, directives and terminology reference

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 the Lembaga Tabung Pekerja	Employees and employers

[43] https://thescoop.co/2020/02/06/brunei-reports-39-rise-in-cyber-attacks-in-2018/
[44] https://www.brudirect.com/news.php?id=73599

Terminology	Definition
Administrator	refers to the e-Government National Centre
Agency/agencies	any government ministry or department including educational institutions and statutory bodies
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 an employee entered into a contract of service or apprenticeship with
Individual	a natural person to whom the data relates, 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.

Cambodia

Cambodia does not currently have any legislation specifically providing for the protection of personal information. Information privacy is covered by sector-specific laws, which contain provisions protecting customer confidential information but do not specify personal information. A law to provide individuals with the right to access their personal information is being drafted. Currently any incidents associated with data protection are reported under the 'right to privacy' and are covered under the Constitution of the Kingdom of Cambodia, 2010, the Civil Code of Cambodia, 2007, and the Criminal Code of the Kingdom of Cambodia, 2009, also known as the Penal Code.

Article 40 of the constitution states that all Cambodian citizens are accorded both protection of their rights due to residency, and confidentiality of correspondence by mail, telegram, telex, facsimile and telephone. International treaties ratified by Cambodia, including the Universal Declaration of Human Rights, 1948 (Article 12) and the United Nations International Covenant on Civil and Political Rights, 1966 (Article 17), generally protect the rights of individuals to privacy. These international treaties are legally binding in Cambodia as mandated by Constitutional Council Decision No. 092/003/2007 dated 10 July 2007.

The Civil Code of Cambodia protects an individual's personal data as part of their personal rights (Articles 10, 11, 12 and 13). In addition, contractual agreements governing personal data also protect an individual's personal rights and their rights related to accessing, obtaining, processing, and commercialising personal data, subject to the data owner's valid agreed consent. The Penal Code of Cambodia prohibits people from intercepting or recording private conversations, or recording a person's image in a private location, without their consent. Consent is presumed to be given if the concerned person does not object to the notification of the interception or recording.

Key considerations:

Proposed cybercrime law: In the latter half of 2020[45] the Cambodian government is expected to introduce a cybercrime law to curb cybercrime in the country. The draft version of the law governs unauthorised access to private information, malicious software, hacking, spam and computer viruses.

Sector-specific regulation: While there is no national comprehensive privacy legislation, there are sector-specific regulations that regulate customer data. In the banking and financial sector, there are laws to prohibit the disclosure of confidential information and provide specific requirements for the correction and security of consumer data[46]

[45] https://www.dataguidance.com/opinion/cambodia-implications-draft-cybercrime-law
[46] https://www.dataguidance.com/notes/cambodia-data-protection-overview

New e-commerce legislation: In November 2019, an e-commerce law was enacted to regulate online electronic transactions. The law took legal effect in May 2020[47] and contains provisions to 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.[48]

Cases

A group of hackers known as 'Temp.Periscope' hacked into several Cambodian organisations before the July 2018 general election.[49] They primarily used phishing emails and software to profile and potentially infect victims' systems.

Relevant laws, directives and terminology reference

Law/regulation or standard	Industry	Regulator	Applicability
Law on telecommunications 2015	Telecommunications	Ministry of Post and Telecommunications	ICT and telecommunications operators
Press Law (1995)	Media	Ministry of Information	Media publishers
Draft law on access to information	Media	Ministry of Information	Public institutions, natural and legal persons
Draft cybercrime law	IT	National Anti-Cybercrime Committee	General public
Law on banking and financial institutions (1999)	Banking and finance	National Bank of Cambodia	Banking and financial institutions
Law on negotiable instruments and payment transactions (2005)	Banking and finance	National Bank of Cambodia	Banking and financial institutions

[47] https://www.dataguidance.com/notes/cambodia-data-protection-overview
[48] https://www.hrw.org/news/2019/12/11/cambodia-access-information-bill-falls-short
[49] https://time.com/5334262/chinese-hackers-cambodia-elections-report/

Law/regulation or standard	Industry	Regulator	Applicability
Law on the management of private medical, paramedical and medical aid profession (2000)	Health care	Ministry of Health Cambodia	Medical professionals Dentists Midwives Nurses Pharmacists
Labour Law (2007)	Labour	Ministry of Health Cambodia	Members of the arbitration panel, labour inspectors, labours physicians and labour supervisors
E-commerce law (2019)[50]	Commerce	National Committee on Consumer Protection	E-commerce operators
Law on the statute of lawyers (1995)	Legal	Bar Association of the Kingdom of Cambodia	Lawyers
Sub-decree on code of ethics for professional accountants and auditors (2005)	Accounting and auditing	National Accounting Council	Professional accountants and auditors

[50] Please note, the e-commerce law is aimed at governing electronic commerce in Cambodia, providing legal certainty in commercial and civil transactions by electronic system, and promoting public confidence in using electronic communication. However, the e-commerce law does not apply to activities, documents and transactions related to: (i) the formation or enforcement of powers of attorney; (ii) the formation or execution of a testament, codicil or other matters relating to succession; (iii) any contract for the sale, transfer or disposition of rights to immovable property or any interests in such immovable property; (iv) the transfer of immovable property or any interests relating to the immovable property; and (v) any other exceptions as provided for by a sub-decree.

China

When operating in China, organisations should be aware of the complexity of the regulatory landscape and rules that vary according to location. There are also sector-specific laws that address the protection of personal information. The protection of personal information in China is regulated by the People's Republic of China Cybersecurity Law 2017 (CSL). The CSL has broad applications and applies to network operators covering most businesses that operate with a computer network, for example an intranet, as well as critical information operators.

As a result of China's rapid adoption of technologies, including Artificial Intelligence (AI) and biometric technology, the Chinese government released a draft Data Security Law[51] for public comment in July 2020. The law aims to introduce rules around markets for data, government data collection and handling, and classification of different types of data.

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

Key considerations:

Law across sectors, provinces and nationally: Organisations are required to adhere to and stay up to date with the obligations prescribed under the laws and regulations of the People's Republic of China. This is an imperative of doing business in China. Guidelines are published to support the laws.

New personal information security specification: The State Administration for Market Regulation and the Standardisation Administration of China issued updated specifications on personal information security practices. These specifications govern aspects including managing third-party access and recording personal information processing activities.[52]

Increasing awareness of privacy rights: The Chinese public have become increasingly aware of their privacy rights, particularly due to high profile court cases. A consumer rights group recently took legal action against a technology company for infringing the rights of its users through collecting excessive personal information without consent.[53]

[51] https://www.davispolk.com/files/2020_07_20_chinas_draft_data_security_law_published_for_public_consultation.pdf
[52] https://www.lexology.com/library/detail.aspx?g=6b467c91-46ca-49e8-adbb-c02c8f490b26
[53] https://www.scmp.com/tech/china-tech/article/2127045/baidu-sued-china-consumer-watchdog-snooping-users-its-smartphone

A new cybersecurity standards practice guide: In March 2020, the National Information Security Standardisation Technical Committee issued a draft consultation paper[54] on the Cybersecurity Standards Practice Guide for Protecting Remote Working Security covering scenarios for remote working, including online meetings, instant messaging, document collaboration, and the creation of a collaborative office. The paper analyses risks associated with remote working, including those over personal information protection, and recommends security control measures for both the organisation and user.

Applications: On 25 January 2019, 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, releasing the Guideline to Self-Assessment of App Collection and Use of Personal Information on 1 March 2019.[55]

New cybersecurity measures:[56] In April 2020, the Cybersecurity Review Measures were released in accordance with the National Security Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China and other laws and regulations. Their aim is to enhance the security and controllability of critical information infrastructure and safeguard national security.

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 in electronic records. Examples of personal information include a person's natural name, date of birth, personal identification information, address and telephone number.

Collection and notice

Network operators must collect personal information:

- legally and in a 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
- with approval and consent of the person to whom the information applies.

On collecting personal information, network operators are required to notify users specifying:

- the purpose of collection
- how the information will be collected
- how the information will be used.

[54] https://www.lexology.com/library/detail.aspx?g=6b467c91-46ca-49e8-adbb-c02c8f490b26
[55] https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/march/31/-/media/ae0259f3ddf14fecb5b3ceb1c25aaec8.ashx
[56] https://amp-scmp-com.cdn.ampproject.org/c/s/amp.scmp.com/news/china/politics/article/3081908/chinas-new-cybersecurity-rules-could-hit-foreign-service

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 for a new purpose, as long as it is voluntary and explicit consent has been sought and 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 deidentified and cannot be recovered.

Data retention and destruction

Personal information must be accurate, 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 practical 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

It is mandatory to notify both the regulator and affected individuals of any data breach.

Requirements	
Threshold for reporting	Where there is a reasonable and 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 • likelihood of identity theft or fraud • ability of users to avoid or mitigate possible harm • reasonable expectation of users' privacy. It is also determined by whether the: • information is adequately encrypted, anonymised or otherwise rendered inaccessible • breach is ongoing and there will be further exposure of personal information • breach is an isolated incident or a systematic problem • information has been retrieved before being accessed or copied • effective mitigation or remediation was conducted after the breach.
Time frame	Network operators should provide a 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 party able to take remedial action to mitigate the impact of the breach.
Content	Depending on circumstances, notification should include: • a general description, including discovery, time and duration of the breach • the source of the breach and types of personal information involved • an assessment of the risk of actual harm • 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 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 China, a security assessment must be conducted in accordance with measures formulated by the Cyberspace Administration of China (CAC).

Governance

The appointment of a Data Protection Officer is not required. However, a network operator or Critical Information Infrastructure Operator (CIIO) must be appointed.

Regulators and regulatory landscape

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

- creating a cyberspace policy
- acting as the central internet regulator
- providing regulatory oversight and censorship.

Cases

- **2020 –** a Chinese bank[57] was fined ¥1.845 million for carrying out a number of illegal activities, including infringing customers' personal information rights. This was due to falsely reporting or concealing financial statistical information and failing to:
  - submit materials on the opening, changing and closing of accounts
  - manage the barcode payment business
  - handle objections in accordance with credit reporting regulations
  - perform obligatory customer identification procedures
  - submit reports on suspicious transactions.

- **2020 –** a Chinese microblogging website issued a statement confirming the sale of data records containing publicly posted information. A user reported finding 538 million data records for sale on the dark web.[58] China's Ministry of Industry and Information Technology issued a statement in March 2020 directed at microblogging websites to strengthen data security measures and notify users and authorities in the event of a data breach.

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.

[57] https://sites-herbertsmithfreehills.vuturevx.com/95/22365/april-2020/china-cybersecurity-and-data-protection--monthly-update---april-2020-issue.asp?sid=acde3402-31d9-4775-827b-63920b62c3f4#three
[58] https://www.zdnet.com/article/hacker-selling-data-of-538-million-weibo-users/

Relevant laws, directives and terminology reference

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	N/A	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	Definition
Critical information infrastructure operators	any industry-related operator, including those in public communication 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, the national economy, and people's livelihood and public interests
Network	any system composed of computers or other information terminals and related equipment, which executes procedures of information collection, storage, transmission, exchange and processing
Network operator	Any owners or managers of the network and network service providers.

Hong Kong

Hong Kong's Personal Data (Privacy) Ordinance (PDPO) is 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 Data Protection Directive with a major reform in 2012 to incorporate additional provisions. Currently, the regulator is reviewing the PDPO[59] in response to multiple data breaches and the changing global privacy regulatory landscape.

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

Key considerations:

International legislation: Given recent international privacy regulations, the PCPD indicated an intention to review its laws to align the PDPO with the EU's GDPR and China's cybersecurity laws in particular.

Review of the PDPO: Following major data leaks and cyber-attacks in Hong Kong, the PCPD is also looking to review the PDPO. No timelines have been announced with the proposed amendments to include a mandatory data breach notification mechanism, clear data retention policy, direct regulation of data processors and increasing penalties for non-compliance.[60]

The review concentrates on:

- a wider definition of personal data to capture identifiable natural persons rather than simply identified ones
- direct regulation of data processors to impose legal obligations on them and possibly subject them to enforcement action for breaches of the new obligations
- introducing a mandatory breach notification regime, obliging data users to notify the regulator and data subjects in the event of a data breach
- enhanced data retention requirements through requesting that data users to develop clear retention policies with specified retention periods for the personal data collected
- more powerful sanctioning powers for the Privacy Commissioner, allowing for the imposition of administrative penalties, including turnover-related fines
- introducing provisions to prevent and deal with doxing (to publicly identify or publish private information about someone, especially as a form of punishment or revenge)[61]

[59] https://www.pcpd.org.hk/english/news_events/media_statements/files/Paper_GroovingPrivacyEvolutionwithDataEthics_Feb2019.pdf
[60] https://www.legco.gov.hk/yr19-20/english/panels/ca/papers/ca20200120cb2-512-3-e.pdf
[61] https://www.merriam-webster.com/dictionary/dox

Definition of personal data

Personal data is defined as information that:

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

The PDPO does not define sensitive data, however, the codes of practice that regulate data include the Hong Kong Identification Card numbers and unique identifiers, including passport numbers and patient numbers. The PCPD issued specific guidance on biometric data, stating that such data can only be collected when necessary and with free and informed consent from the data subject.

Collection and notice

Data must be collected:

- in a lawful and fair manner
- directly related to an activity of the data user
- if necessary, but not excessively for the related purpose.

Organisations must inform an individual whether it is mandatory to provide their data and the consequences of not doing so. They must also notify them why, the purpose of collection and its 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 to be used or disclosed for a purpose other than that for which the data was originally collected or a directly related purpose, prescribed consent must be obtained from the data subject. Prescribed consent is consent given voluntarily and that 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. 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 must be informed:

- if their information is to be used for direct marketing
- of the types of data that will be used
- as to the purpose of the marketing
- about how to communicate consent for the intended use
- that 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 accurate and kept up to date. It should be kept no longer than necessary to fulfil the purpose for which it is collected. The PDPO requires data users to take all practical steps to erase personal data that is no longer required for the original purpose for which the data was collected, unless erasure is prohibited by law or is not in the public interest.

Individual rights

Data subjects have the right to:

- **be informed** of their rights at, or prior to **collection and use** of their data
- be informed of the **retention** period, the security measures in place to protect their data and how to raise an access and correction request
- **access** and **correct** their personal data.

Organisations must respond to access or correction requests within 40 days or inform the individuals that they are unable to do so within the timeframe.

Security

Organisations must take practical steps to protect personal data from unauthorised or accidental access, processing, erasure, loss or use. Factors to consider include the:

- kinds of data held
- potential harm if the data is inadequately protected
- security measures incorporated into data storage equipment
- secure transmission of data
- physical location of the data storage
- measures for assuring the integrity, prudence and competence of people who can access the data.

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 PCPD has recommended voluntary notification in the event of a data breach via the Guidance on Data Breach Handling and the Giving of Breach Notifications.[62]

[62] https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

Voluntary guidance	
Threshold for reporting	If there is a reasonably foreseeable and real risk of harm or damage from the breach, depending on the: • kind of personal data leaked • amount of personal data involved • circumstances of the data breach • likelihood of identity theft or fraud • ability of data subjects to avoid or mitigate possible harm • reasonable expectation of personal privacy of the data subjects involved. Or whether the: • leaked data is adequately encrypted, anonymised or otherwise rendered inaccessible • data breach is ongoing and there will be further exposure of data • breach is an isolated incident or a systematic problem • effective mitigation or remediation was conducted after breach • case was of physical loss and personal data was retrieved before it was accessed or copied.
Time frame	As soon as practicable, except where law enforcement agencies have requested a delay for investigative purposes.
Who to notify	Depending on circumstances including: • affected data subjects • law enforcement agencies • the PCPD • relevant regulators • other parties able to take remedial actions to mitigate the impact of the breach.
Content	Depending on circumstances to include the: • general description • date, time and duration of the breach • date and time when the breach was first discovered • source of the breach • types of personal data involved • assessment of risk of harm from the breach • description of measures taken to prevent a continued breach • organisation's contact information for more information and assistance • information and advice on further steps data subjects should take • fact that the law enforcement agencies, PCPD and other parties have been notified.

Cross-border data transfer

Organisations can only transfer personal data if data subjects were initially informed when their personal data was collected that their data may be transferred and the classes of people to whom it may be transferred.

The PDPO prohibits cross border transfers of data except in specified circumstances. That provision is yet to be enacted. The PCPD currently provides a Guidance on Personal Data Protection in Cross-border Data Transfer to outline best practices for the cross-border transfer of data. This recommends organisations review data transfer agreements and keep an inventory of personal data.

Governance

There is no mandatory requirement to appoint a data protection officer. However, the PCPD advocates companies be accountable for the protection of personal data to build trust with clients, enhance reputation and increase competitiveness.

Regulators and regulatory landscape

The 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
- promoting education, training and best practice
- corporate governance
- meeting changing needs relating to technological developments, trends and expectations.

Cases

- **2020 :** A broadband network company pleaded guilty to six charges under the PDPO to using the personal data of a data subject in direct marketing without obtaining the data subject's consent, and failing to comply with the requirement from the data subject to cease using their personal data in direct marketing. The company was fined HK$12,000 in total (HK$2,000 for each charge).[63]
- **2019 :** The first doxing and cyberbullying case was received by the PCPD on 14 June 2019. As of 21 October 2019, the PCPD received and proactively found a total of 2,683 related cases, in which 13 online social platforms and discussion forums and 2,145 web links were involved.[64]
- **2019 :** A telecommunications company was fined HK$84,000 in September 2019, charged with failing to comply with requirements from the data subject to cease using their personal data in direct marketing, contrary to section 35G(3) of Personal Data Privacy Ordinance.[65]

Exemptions[66]

The PDPO provides a number of exemptions including crime prevention or prosecution, security and defence, statistics and research, news activity, protecting a data subject's health, and where the use of personal data is required or authorised by law or court order, or to exercise or defend the legal rights in Hong Kong. Exemptions are also provided for conducting due diligence exercises in connection with proposed business transactions.

[63] https://www.pcpd.org.hk/english/media/media_statements/press_20200525.html#:~:text=HKBN%20was%20fined%20HK%2412%2C000,in%20respect%20of%20each%20charge).&text=The%20case%20concerned%20a%20complaint,Kong%20(PCPD)%20in%202018.

[64] https://www.pcpd.org.hk/english/media/media_statements/press_20191021.html

[65] https://www.pcpd.org.hk/english/media/media_statements/press_20190912.html

[66] Section 53A to 63D, PDPO

Penalties

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

Section 26 of PDPO provides that when a data user fails to respond to a complaint or request from a data subject to erase their personal data, the data user could be fined up to HK$10,000.[67]

If a data user fails to inform its data subjects as to the intention, classes of marketing and scope of gaining profits through its direct marketing activities conducted in lieu of transferring data to a third party, the user may be fined HK$500,000 and imprisoned for three years. Or, if the data was provided to a third party for gain, issued a fine up to HK$1,000,000 and imprisonment for five years.

Relevant laws, directives and terminology reference

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 & finance	HKMA	Authorised institutions under the banking ordinance
Code of practice on consumer credit data	Banking & finance	PCPD	Credit providers and credit referencing agencies
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

[67] https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html?f=486

Terminology	Definition
Data users	a person who, either alone, 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
Codes of practice	practical guidance as to requirements under the PDPO
Guidelines and circulars	the information provided in this guidance note is for general reference only. Letters or guidance are distributed to industry reminding them of regulatory requirements and clarifying regulatory issues.

India

A standalone privacy law does not yet exist in India. However, the Information Technology Act 2000 (IT Act) presently governs the protection of personal information, specifically electronic data and transactions. The prominence of data use has elevated privacy and data protection up the national agenda and is recognised as a key to India's growth and economic development. The government demonstrated its interest in creating a digital health technology ecosystem for instance, releasing the draft Digital Information Security in Healthcare Act (DISHA) aimed at regulating the process of collection, storing, transmission and use of digital health data. Additionally, in August 2015, the Prime Minister of India announced the launch of the National Digital Health Mission (NDHM), which will create an ecosystem with four key features - health ID, personal health records, Digi Doctor and health facility registry.[68]

In 2018, the government of India's Ministry of Electronics and Information Technology (MeitY) constituted a committee of experts under the chairmanship of Justice B.N.Srikrishna (a former judge at the Supreme Court of India) to formulate a bill on personal Data Protection (PDPB 2018).[69] Following the formulation of PDPB 2018 in December 2019, a Personal Data Protection Bill, 2019 (PDPB)[70] was introduced in the lower house of Parliament. Once enacted in its current form, the PDPB will require a significant number of companies, both Indian and foreign, to revamp their operational practices in relation to data processing and embed practices and technologies to enable privacy and protection of data within their systems.

Primary legislation: Information Technology Act, 2000

Key considerations:

Constitutional right to privacy:[71] The Supreme Court in 2017 delivered a judgment in relation to the constitutional right to privacy which remains legal grounds today – that is 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 their personal data. As a result, there is an obligation to ensure the protection of a citizen's right to privacy.

[68] https://www.nhp.gov.in/national-digital-health-mission-(ndhm)_pg
[69] https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[70] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[71] https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Key features of the PDPB: The PDPB (2019 version) updates the Draft PDPB 2018 and includes:

- **The right to be forgotten:** PDPB gives a data principal, the natural person to whom the data relates, the right to be forgotten. This is to stop their data from being disclosed if the purpose of data collection has been served, or they withdraw consent, or the data was disclosed contrary to provisions of PDPB. The data principal will have to make a complaint to an adjudicating officer in this regard. The data principal can make a complaint to the Data Protection Authority (DPA) to order the data fiduciary to remove their personal data
- **Significant data fiduciaries:** The DPA can declare any data fiduciary as being a significant data fiduciary on the basis of the volume and sensitivity of personal data being processed, the data fiduciary's turnover, any risk of harm by processing and/or its use of new technologies for processing
- **Social media intermediaries:** Social media intermediaries are entities that enable online interaction between two or more users and let them create, upload, share, disseminate, modify or access information using their services. They will have a high volume of users and the ability to impact electoral democracy, India's security, sovereignty or public order, and can be classified by the central government and DPA as a significant data fiduciary. Social media intermediaries, classified as significant data fiduciaries, will have to provide account verification options to willing data principals. The verification has to be a visible mark with its form and manner yet to be codified by the central government and it must be voluntary
- **Data localisation:** There is currently no restriction transferring personal data such as name and contact number outside India. However, sensitive personal data such as financial and health data must be stored in India and can only be transferred for processing outside India with the principal's explicit consent and the DPA's or Central Government's permission, or pursuant to a contractual obligation. 'Critical' personal data, a term yet to be formally defined, can only be stored in India and its transfer is restricted
- **Regulatory sandbox:** A regulatory sandbox has been proposed to enable the development of new technologies for AI and machine learning. Sandboxing will extend exemptions to qualified entities from purpose, storage and consent requirements under PDPB
- **Consent managers:** A consent manager is defined as a data fiduciary, which enables a data principal to gain, withdraw, review, and manage their consent through an accessible, transparent, and interoperable platform. Individuals may use the consent manager platform to give or withdraw their consent from the data fiduciary.

Non-personal data:[72] In July 2020 the MeitY committee released its report on non-personal data (NPD) governance framework. The committee recommended a separate legislation be formulated to govern NPD, a new regulatory body be constituted for governing matters related to NPD and for NPD to be categorised into public, community and private NPD. The report has defined NPD as data that never related to an identified or identifiable natural person, such as data on weather conditions, from sensors installed on industrial machines, from public infrastructures, or data that was initially personal data but later anonymised.

[72] https://www.prsindia.org/report-summaries/non-personal-data-governance-framework#:~:text=In%20terms%20of%20origin%2C%20non,relates%20to%20cannot%20be%20identified).

Definition of personal data

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 that is 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 and 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 programmes 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 IT 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 systems or networks
- actions taken to mitigate damage
- other relevant technical information, such as the security systems used.

Cross-border data transfer

Where required by law, under contract or with consent, organisations can transfer sensitive information to receivers adhering to the same level of data protection.

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. They can impose penalties.

Cases

- **2020 –** an Indian hyperlocal delivery service suffered a data breach that left customer data including email IDs and phone numbers exposed.[73]
- **2020 –** the Kerala High Court held that the Government of Kerala must anonymise the COVID-19 related data it had collected through software provided by Sprinklr. The court added that the Government of Kerala is obliged to inform every citizen from whom data is to be taken in the future, that such data is likely to be accessed by Sprinklr or other third-party service providers and their specific consent needs to be obtained in the necessary format.[74]
- **2019 –** the Kerala High Court held that the right to have access to the internet is part of the fundamental right to education, as well as the right to privacy under Article 21 of the Constitution.[75]
- **2019 –** the data of approximately 300 million Indian users on a Swedish mobile application platform was leaked and made available for sale on the dark web.[76]

Penalties

Breach of confidentiality and privacy under the IT Act is punishable with an imprisonment of up to two years and a fine up to ₹100,000 or both. Disclosure of information in breach of a lawful contract is punishable with imprisonment of up to three years and a fine up to ₹500,000 or both.

[73] https://thenextweb.com/in/2020/07/11/google-backed-indian-delivery-startup-dunzo-suffers-data-breach/
[74] http://highcourtofkerala.nic.in/covid_files/WTPTMP841321481632020240420 20.pdf
[75] https://sflc.in/kerala-high-court-declares-right-access-internet-fundamental-right
[76] https://analyticsindiamag.com/data-breaches-faced-by-indian-consumer-internet-companies-in-2019/#:~:text=Truecaller,sale%20on%20the%20dark%20web.&text=However%2C%20when%20asked%2C%20Truecaller%20said,of%20leak%20in%20the%20information.

Key laws, directives and terminology reference

Law/directive	Industry	Regulator	Applicability
The Information Technology (reasonable security practices and procedures and Sensitive Personal Data or Information) Rules, 2011[77]	Information technology and communications	The Central Government of India	Body corporates and persons in India
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	Indian government and private e-commerce entities
The Storage of Payment System Data Directive, 2018	Finance	The Reserve Bank of India	Payment system providers
DISHA (Digital Information Security in Healthcare Act, 2018)	Health care	The Ministry of Health and Family Welfare	Individuals, health care providers, clinical establishments and hospitals
IRDAI (maintenance of insurance records) Regulations, 2015	Insurance	The Insurance Regulatory and Development Authority of India (IRDAI)	Individuals and insurance providers
Aadhaar (targeted delivery of financial and other subsidies, benefits and services) Act, 2016 **Aadhaar and Other Laws (Amendment) Ordinance, 2019** **The Aadhaar and Other Laws (Amendment) Act, 2019**	National identification	Unique Identification Authority of India (UIDAI)	Individuals, private organisations, public organisations, enrolment agencies, Aadhaar Seva Kendra, authentication requesting and authentication service agencies.

[77] https://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.

Terminology	Definition
Data principal	the natural person to whom personal data relates
Data fiduciary	any person, state, company, juristic entity or individual who alone or in conjunction with others, determines the purposes and means of personal data processing
Data processor	any person, state, company, juristic entity or individual who processes personal data on behalf of a data fiduciary but does not include an employee of a data fiduciary
Consent manager	a data fiduciary, that enables a data principal to gain, withdraw, review and manage their consent through an accessible, transparent and interoperable platform
Social media intermediary	an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services, but shall not include intermediaries which primarily: • enable commercial or business-oriented transactions • provide access to the internet • are in the nature of search-engines, on-line encyclopaedias, e-mail services or online storage services
Authentication requesting agency	an agency or a person that submits Aadhaar number and demographic information or biometric information, of an individual to the Central Identities Data Repository (CIDR) for authentication
Authentication Service Agency (ASA)	agencies that have established secured leased-line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to requesting entities (such as AUAs/KUAs) and transmit their authentication requests to CIDR
Data Protection Authority	the regulatory body tasked with regulating the provisions of PDPB, to frame regulations on issues such as data collection, consent taking mechanisms, data use limitations, and cross-border data transfer and adjudicating grievances
Intra-group schemes	contractual frameworks governing an organisation to facilitate free and secure transfer of data between various subsidiaries and/or regional offices of a parent organisation.

Indonesia

Indonesia does not currently have formalised laws to regulate the privacy and data protection of individuals. Instead, privacy and data protection are governed by provisions across a set of regulations that include:

- Government regulation no. 71 of 2019 (GR 71/2019)
- Law no. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its amendment law no. 19 of 2016
- MOCI regulation no. 20 of 2016 (Protection of Personal Data in an Electronic System) (MOCI Law)

These regulations only apply to personal data on electronic systems. A draft data protection law, the Bill on Protection of Personal data (PDPB) that applies to both electronic and non-electronic formats of data, has been officially submitted by the President of Indonesia to the Indonesian House of Representatives. The PDPB is included as a prioritised bill within the 2020 National Legislation Program, a list setting out prioritised draft legislations, and was due to be released by November 2020.[78]

Key considerations:

The two types of personal data are:

- **general:** the basic information about an individual, including his or her name, gender, nationality, religion, and combined personal data that identifies a person
- **specific:** a person's health data and information, biometric data, genetic data, sexual orientation, political view, criminal record, children's data, private financial data and/or other data specified under the prevailing laws and regulations.

When processing personal data, the PDPB requires it is:

- lawful and purpose-oriented
- securely conducted to protect it from unauthorised access, disclosure and alteration
- written or has verbal consent

[78] https://www.privacylaws.com/news/indonesia-s-protection-of-personal-data-bill-introduced-into-the-legislature/

The PDPB specifies an individual's rights to protect their personal data includes the right to:

- be informed
- access personal data
- rectify and erase personal data
- withdraw from processing activities
- claim damages in case of personal data breach.

Personal data transfer cross-border: Permitted to a country or international organisation with an equal or higher level of personal data protection compared with Indonesia. In addition:

- parties can use contracts to protect personal data transfers
- individual consent may also be obtained to transfer personal data internationally
- unlawful processing of personal data attracts penalties ranging from Rp20 billion to Rp70 billion and/or imprisonment ranges from two to seven years.

The national regulating authority: The Ministry of Communication and Informatics (MOCI) is currently the main regulatory body that oversees data protection activities within Indonesia. Currently there is no formalised privacy regulator. The draft data protection law introduces a Commission with functions and powers to help ensure the protection of personal data.

Primary legislation: MOCI Regulation No. 20 of 2016 (Protection of Personal data in an Electronic System) (MOCI Law)

Definition of personal data

Personal data is defined as individual data that is stored, maintained and accurate. 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 to collect, use, process and transfer personal data. Consent must be in writing and provided manually or electronically. An electronic system provider must provide a consent form prior to collection. Parents or legal guardians can provide consent in cases, such as minors or disabled persons, where the individual is not capable of providing consent.

- Notice must be provided to individuals when the personal data is collected. The notice should include:
  - details on the current and possible future purposes for collection of personal data
  - the organisation's contact details.

Use and disclosure

Personal data can only be used and processed according to the purpose provided in the notice when the personal data was collected. It 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 must be deleted when the storage period provided at the time of collection expires, unless it is still required for the intended purpose, or the data owner has requested it be deleted.

Individual rights

Individuals have the right to:

- **complain** to the MOCI on 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 in both Gov. Reg.71[79] and the MOCI Reg. 20.[80] Broadly, regulations impose an obligation for organisations to obtain certification of their electronic systems to ensure compliance and maintain the correctness, validity, confidentiality, accuracy, relevance and compatibility with the original purpose of the personal data collection.

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
- details of the recipient
- details about the transfer itself, including the intended date and purposes of the transfer.

Consent must also be obtained for the 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. Any 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.

[79] https://www.lexology.com/library/detail.aspx?g=cd6e5251-6dd7-4b46-b6be-759c78c9bf7b
[80] http://makna.co/wp-content/uploads/2018/01/MOCI-Regulation-No-20-of-2016-Makna-Eng.pdf

Notification requirements	
Threshold for reporting	The operator must notify individuals if the breach has potential to cause loss to the individual and 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.[81] And it must notify the relevant authority of the sector in which it operates immediately.
Who to notify	Electronic system operators must notify: • data subjects • law enforcement or the supervising and regulatory authority of the relevant sector.
Content	The operator is to provide affected individuals the cause of the personal data breach in writing unless the individual consented to electronic communication at the point of collection.

Governance

There is no requirement to appoint a Data Protection Officer.

Regulators and regulatory landscape

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

Cases

- **May 2020:** a leading Indonesian e-commerce firm was subjected to a data breach, jeopardising more than 15 million user accounts. The compromised database contains emails, passwords and names, and the data was allegedly sold for US$5,000 online.[82]

Penalties

Breaches of the MOCI reg. or reg. 71 will attract administrative sanctions, including 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.

[81] MOCI Regulation Article 28(c)
[82] https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html#:~:text=A%20recent%20data%20breach%20jeopardizing,meet%20their%20needs%20from%20home.

Relevant laws, directives and terminology reference

Law/Directive	Industry	Regulator	Applicability
Government Regulation No. 71 2019	Comprehensive	Ministry of Communications and Informatics	Electronic system operators
MOCI Regulation No. 20 of 2016 (Data Protection Regulation)	Comprehensive	MOCI	Electronic system operators
Law No. 11 of 2008 on Electronic Information and Transactions and its amendment Law No. 19 of 2016	Comprehensive	The Indonesian government	Electronic system operators
Draft of Personal Data Protection Act (PDPB)	Comprehensive	Indonesian Government	Comprehensive
Regulation for the Financial Services Authority on Consumer Protection in the Financial Service Sector, 2013 (POJK)	Financial institutions	Financial Services Authority	Comprehensive
Law on Health No. 36/2009	Health	Ministry of Health	Health providers

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.

Japan

In Japan privacy is regulated by the Act on the Protection of Personal Information (APPI) which came into force in 2005 and was subsequently amended in 2017 and 2020. 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.

Primary legislation: Act on the Protection of Personal Information (APPI)

Key considerations:

Amendment Bill:[83] On 10 March 2020, the cabinet passed the Amendment Bill to the APPI, and submitted it to the ongoing ordinary session (201st session) of parliament on the same day.[84] The Amendment Bill focused on the individual rights of a principal, the obligations of business operators, penalties, data utilisation and cross-border data transfer. On 5 June 2020, the Bill was passed, amending the Protection of Personal Information Act (Act No. 57 of 2003 as amended in 2016) [Amended APPI]. The Amended APPI will come into force no later than two years after its promulgation.

EU adequacy: On 23 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 has created, developed and facilitated opportunities for European and Japanese businesses to share data. The decision was supported by supplementary rules that strengthened the APPI, including additional protection for new types of sensitive personal information (special care required).[85]

Japan's Fair Trade Commission (FTC) is considering regulating data that is comparable to personal information, such as cookies, with a guideline released in December 2019. The need to create this guideline arose from the possibility that companies may be violating the Anti-Monopoly Law if they use data that is comparable to personal information outside the principal's intention.[86]

[83] https://www.ppc.go.jp/en/
[84] https://www.ppc.go.jp/files/pdf/amendment_bill202003.pdf
[85] https://ec.europa.eu/info/sites/info/files/annex_i_supplementary_rules_en.pdf
[86] https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217_DP.html

Definition of personal information

Personal information is defined as information that relates to a living individual and can contain:

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

The APPI also defines special care required personal information (sensitive information) to include personal information comprised 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. They must promptly and explicitly inform the principal of the purpose of the personal information acquisition, and where the purpose has changed. This requirement does not apply where there exists an urgent need to protect human life, body or fortune, or where the purpose was previously disclosed to the public. PIHBOs must obtain the principal's consent before collecting sensitive information unless:

- 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 obtaining the principal's consent would interfere with this
- the information is publicly 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 apply. For example, where the purpose requires providing personal information to a third party.

As a way of helping to promote innovation while protecting privacy, the Amended APPI introduces the concept of Pseudonymously Processed Information, which is where certain details of a person's name etc. are deleted from personal information. The Bill also provides for obligations with regard to a principal's rights and data breach notification. It also permits internal use of pseudonymously processed information by a personal information controller (PIC) beyond the purpose of use, published or notified to principals.

The Amended APPI does not allow the **opt-out exception for third-party consent** to be used for:[87]

- personal data which was improperly collected (i.e. violating Article 17 of the APPI)
- personal data transferred from a third party using the same opt-out exception may not be transferred using the opt-out exception.

[87] https://www.lexology.com/library/detail.aspx?g=708ce496-e027-45c0-9d62-105cdd9e8d6a

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 endeavour to delete personal information, without delay, once its purpose has been fulfilled. Industry codes and standards also specify requirements for the retention and destruction of personal information.

Individual rights

Individuals have the right to:

- request **disclosure**, **rectification** and/or **erasure** of their personal information held by PIHBOs because their personal information is incorrect
- **object** to processing by lodging a use cease request, based on reasonable grounds
- lodge **complaints** to the PPC or any other authorised entity about the handling of their personal information.

The amended APPI suggests changing individual rights to:[88]

- broaden principal **rights to erasure and restriction of processing** if it becomes unnecessary for the PIC to process personal data, or if a PIC fails to process personal data in a proper manner or is likely to infringe a principal's rights or legitimate interests
- enable principals, under their **right to access and right to data portability** to demand the PIC disclose, by electronic means, what personal data the PIC has on them.

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.

Data breach notification

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

The amended APPI introduces **mandatory obligations to report data breach incidents** to the PPC and notify the affected principals.

[88] https://www.ppc.go.jp/en/

Voluntary guidance	
Threshold for reporting	Where there is a reasonable, foreseeable real risk of harm or damage from breach depending on the: • kind and amount of personal information leaked • circumstances of data breach • likelihood of identity theft or fraud • ability of principals to avoid or mitigate possible harm • reasonable expectation of a principal's personal privacy. Or reasonable, foreseeable real risk of harm or damage from breach whether: • leaked information is adequately encrypted, anonymised or otherwise rendered inaccessible • the data breach is ongoing and there will be further exposure • the breach is an isolated incident or a systematic problem • personal information in case of physical loss, was retrieved before being accessed or copied • effective mitigation or remediation was conducted after the breach.
Time frame	As soon as practicable, except where law enforcement agencies have requested a delay for investigative purposes.
Who to notify	Electronic system operators must notify: • affected data subjects • the Commissioner • relevant regulators or law enforcement agencies • parties that 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.

Cross-border data transfer

Personal information must not be transferred to a third party unless consent has been obtained from the principal or where any of the exceptions to consent being required apply.

Personal information may be transferred outside Japan where:

- consent is obtained from the principal
- the foreign state has privacy laws considered to be equivalent to Japan
- the foreign party maintains an internal personal information protection system consistent with standards set by the PPC
- the EU Adequacy decision applies allowing free flow of data between EEA (European Economic Area) and Japan without being subject to any further safeguards or authorisations.

The following changes have been made in the amended APPI:[89]

- foreign business operators that supply goods or services in Japan and handle personal information of an individual in Japan will be subject to reports on handling personal information and orders. Penalties, if applicable, made by the competent minister of the relevant business/sector/industry handling the said personal information, will apply.
- when transferring personal data to a third party in a foreign country, a business operator will be required to provide information to the principal as to how the third party manages their personal information, including details on processing, retention periods, secure destruction practices and technical safeguards.

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
- reporting.

Cases

- **February 2020:** The Japan Ministry of Defence announced that defence-related sensitive data, as well as particular personal information, may have been breached after the cyberattack on a major supplier of the country's defence and infrastructure systems.[90]
- **2019:** A car manufacturer publicly notified a data breach caused by third party attackers through its dealerships. The breach was limited to unauthorised access of computer systems, and led to compromised personal information of more than 3.1 million customers, including names, birth dates and employment information.[91]

[89] https://www.ppc.go.jp/en/
[90] https://www.cpomagazine.com/cyber-security/major-japanese-defense-contractors-admit-to-data-breach-incidents-dating-back-to-over-four-years-ago/
[91] https://www.cpomagazine.com/cyber-security/new-toyota-data-breach-exposes-personal-information-of-3-1-million-customers/

Exemptions

The APPI exempts:[92]

- broadcasting institutions, newspaper publishers, communication agencies and other press organisations (including individuals engaged in the press as their business) with its purpose being to use in the press
- persons who write as a profession with its purpose being to use in writing
- universities and other organisations or groups aimed at academic studies, or persons belonging to them with the purpose to be used in academic studies
- religious bodies with the purpose to be used in a religious activity (including accessories to those activities)
- political bodies with the purpose to be used in a political activity (including accessories to those activities).

Penalties

Per the APPI, penalties for business operators can include:

- up to one year's 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 violating an order from the PPC
- up to six months' imprisonment, or a maximum fine of ¥300,000 for failing to submit a report on request or providing false reports to the PPC.

Penalties may also apply to business operator's representatives, such as an individual employee.

Per the amended APPI, the following changes to penalties will take place:

- imprisonment with labour of up to one year, or a maximum fine of ¥1 million for an individual violating an order from the PPC
- a fine of up to ¥500,000 for false submission of a report
- a fine up to ¥100,000,000 for PIHBO's disclosing personal information for illegal profit or PIHBO's violating an order from the PPC.

[92] Article 76, APPI

Relevant laws, directives and terminology reference

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 & 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	Definition
Individual identification code	prescribed by cabinet order to include any character, letter, number, symbol or other codes 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 legal person providing a personal information database for use in business but excludes a central government organisation, a local government and an incorporated administrative agency (local or not)
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.

Lao People's Democratic Republic

Lao People's Democratic Republic (Lao PDR) does not currently have a comprehensive data protection and privacy law in place. However, Lao PDR has enacted laws with provisions governing aspects of personal data protection. The Law on Prevention and Combating Cyber Crime 2015[93] (Cybercrime Law) governs monitoring, inspecting and prevention with respect to cyber-crimes, database systems, server systems, computer data and information.

The comprehensive Law on Electronic Data Protection 2017 (EDPL) details requirements to protect personal information and covers collecting, storing, maintaining, using, disseminating, transferring, accessing, amending, updating and deleting electronic data. In August 2018, the Ministry of Posts and Telecommunications (MPT) issued guidelines on implementing the EDPL to cover data collection, electronic data inspection, and how to save, store, maintain, use, disseminate, transmit, transfer, access, amend, update and delete electronic data.[94]

Primary legislation: The Law on Electronic Data Protection (EDPL)

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 when authorised 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 the collected personal data where the data owner has approved such a purpose, unless required otherwise by law.

Data retention and destruction

A data administration authority must delete electronic data once its original purpose has expired or if the data owner requests it be deleted. Data owners must be informed of their record's deletion. A data administration authority has the right to delete personal data if it relates to the stability of the nation, peace and orderliness of the society and has information that may defame an individual.

[93] https://www.laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf
[94] https://www.ela.law/Templates/media/files/Newsletter_Articles_Clients/AP/October/Ministry_of_Posts_and_Telecommunications_Guidelines_Shed_Light_and_Clarity_on_the_Lao_PDR%E2%80%99s_Data_Protection_Regime.pdf

Individual rights

Individual rights
Data owners have the right to:

- **request access** or updates to their personal data
- **request deletion** of their personal data
- **inform** the data administration authority to secure their personal data where the data has been damaged or is at risk
- **complain** to relevant organisations that have collected their data.

Transferring data

A data administration authority cannot share the personal data they collect, maintain or administer with a third person or party without the approval of the data owner, or the mandate of a relevant authorised government organisation.

Sending or transferring electronic data
To send or transfer electronic data, the sender needs to:

- obtain permission from the data owner
- ensure the receiver is able to secure the data it receives
- implement data security measures for important data types such as financial, banking, investment and accounting data
- refrain from falsifying data sources that have been sent and transferred
- maintain consistency with the agreement between the sender and receiver of the data
- refrain from sending or transferring data where the data receiver objects to such transfers.

Individuals, legal entities and organisations cannot send or transfer personal data and official data outside the Lao PDR without permission from the data owner or if doing so contravenes the provisions of EDPL.

Security

A data administration authority must maintain the security of its information and network systems to protect data by:

- using technical systems or tools to secure the data
- inspecting and evaluating risks to data systems on an annual basis
- investigating incidents that have caused or may cause serious impact to the rights of data owners regarding their personal data.

Regulators and regulatory landscape

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

Penalties

Penalties include:

- warnings to and re-education of the violator
- disciplinary action for offences committed by government officials
- a fine of ₭15 million for engaging in a prohibited action which does not constitute a criminal offence
- a potential civil liability for incurred damage
- applying criminal sanctions based on the seriousness of the wrongful act.

Relevant laws, directives and terminology reference

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	Definition
Data owner	the individual, legal entity or organisation that owns the electronic data
Data administration authority	an individual, legal entity or organisation that maintains, uses, discloses, secures and transfers personal data
Electronic data administration authorities	the individual, legal entity or organisation responsible for administrating the electronic data, which are mainly ministries, data centres, telecommunication service providers and banks.

Malaysia

Malaysia is governed by a comprehensive Personal Data Protection Act 2010 (PDPA). The PDPA is principles-based and applies to individuals who process and control, 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) or credit reporting agencies.

The Personal Data Protection Commissioner issued Public Consultation Paper No. 01/2020[95] for consideration in February 2020 to collect feedback on proposed changes to update the PDPA. The areas of change under consideration include data processor obligations, the right to data portability, appointment of Data Privacy Officers (DPOs), data processors with direct obligations to the PDPA, mandatory data breach notifications, the processing of personal data in cloud computing and 'privacy by design'. The PDPA review is being conducted to align with global legislation including the EU's General Data Protection Regulation (GDPR).

Primary legislation: Personal Data Protection Act 2010 (PDPA), Personal Data Protection Standard 2015

Key considerations:

Data user registration: There are 13 classes of data users that need to register under the PDPA before they can process personal data. However, Consultation Paper No. 01/2020 suggests that data users outside these 13 categories should also register. Currently, the data users that require registration come under key industries including communications, banking and financial institutions, insurance, health, tourism and hospitality, transportation, education, direct selling, services, real estate, and utilities. Registration certificates are valid for one year only after which they must be renewed. Registration must be on the website[96] and maintained for this purpose.

Data breach and cross-border transfers: The Malaysian Personal Data Protection Commissioner has issued two public consultation papers covering implementing a data breach notification scheme into the PDPA , and including cross-border data transfer requirements and introducing a data protection officer.

[95] https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf
[96] https://daftar.pdp.gov.my/login.php

Definition of personal data

Personal data includes any information that:

- relates, directly or indirectly, to a data subject
- identifies or enables a data subject to be identified from, either alone or in combination with other information possessed by the data user.

Sensitive data is personal data which comprises:

- information about the physical or mental health 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, and directly related to 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:

- types of data collected
- the purpose of collection
- information about the source of the personal data
- the data subject's rights to access, request correction to and lodge complaints over their personal data
- any disclosure of their personal data to third parties, and if so, to whom
- ways to limit the use and processing of their personal data
- voluntary supply of the data and any consequences if their data is not provided.

Use and disclosure

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

Processing personal data can occur to:

- enter or intend to enter into a contract which the data subject is a party to
- comply with any other legal obligation
- protect the interest of the data subject
- administer justice.

Data users should not process sensitive personal data of a data subject except when:

- the data subject has given explicit consent to processing their personal data
- processing is necessary to exercise or perform any right or obligation, which is conferred or imposed by law on the data user in connection with employment
- protecting the vital interests of the data subject or another person where consent cannot be given by or on behalf of the data subject or the data user cannot reasonably be expected to obtain the consent of the data subject
- protecting the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld, for medical purposes, for the purpose of, or in connection with, any legal proceedings, for the purpose of obtaining legal advice, for the purposes of establishing, exercising or defending legal rights and for the administration of justice.

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. As per the Public Consultation Paper No. 01/2020, the data user is allowed to disclose personal data for a purpose other than that consented to at the time of collection when that purpose is to prevent a crime or an investigation is authorised and required by law or court order.

Data retention and destruction

Data users are responsible for taking reasonable steps to ensure that data processed for any purpose shall not be kept longer than necessary to fulfil that purpose. The personal data needs to be either destroyed or permanently deleted once it is no longer required for the purpose for which it was collected.

Individual rights

Data subjects have the right to:

- **be informed** of their rights prior to collection and use of their personal data
- **access and correct** their personal data held by the data user. Per section 31 of the PDPA, a data user must comply with a data access request within 21 days from the date of receipt
- **withdraw consent** to data processing e.g. data subjects may prevent processing where it is likely to cause damage or distress, or where the processing is for direct marketing purposes
- **prevent** the processing of their personal data where it is likely to cause damage or distress
- prevent processing for the purposes of **direct marketing.**

As per consultation paper No. 01/2020, the right of data portability is one of the suggested additions to the list of rights in the PDPA. This will give individuals the right to obtain and reuse their data for other purposes across different services. Another suggestion is the right of a data subject to know the identity of the third party to whom their personal data has been or is to be disclosed.

Security

Data users are required 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. Data users should also provide sufficient guarantees to data subjects regarding the technical and organisational security measures that will govern the data processing.

Cross-border data transfer

Personal data cannot be transferred outside Malaysia unless otherwise provided by the Minister on 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
- the 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
- the transfer is necessary to protect the vital interests of the data subject or is within the public interest as determined by the Minister.

As per consultation paper No. 01/2020, a guideline will be issued on the mechanism and implementation of cross border data transfers.

Regulators and regulatory landscape

The Personal Data Protection Department (PDPD), led by the Personal Data Protection Commissioner, and the Malaysian Communications and Multimedia Commission (MCMC), led by the Minister, jointly hold responsibility as regulators for privacy and data protection in Malaysia.

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

- **September 2019 :** The personal data of the customers of Malaysian Airlines was stolen from its development centre.[97] The data was stolen in India by a former employee of an e-commerce service provider. The breach was contained as the source was identified and no payment details of customers were leaked.
- **February 2019 :** A Malaysian university reported a data breach of personal data of one million students.[98] The data was leaked online and included personal details of students and alumni enrolled in the university between 2000 and 2018.
- **2020 :** A Malaysian private employment agency was charged and fined RM10,000 for failing to register as a data user and processing personal data without a certificate of registration.
- **2020 :** A Malaysian private higher educational institution was charged for failing to register as a data user and processing personal data without a certificate of registration. A fine of RM10,000 (and in default, three months' imprisonment) was imposed.
- **2020 :** A hotel was charged for failing to register as a data user and processing personal data without a certificate of registration. A fine of RM10,000 (and in default, eight months' imprisonment) was imposed.

Penalties

Violations of the PDPA are punishable with criminal liability and can include fines and/or imprisonment, depending on the section of the Act being breached. Where the processing of personal data does not comply with the Personal Data Protection Principles, punishment of a fine up to but not exceeding RM300,000 may be imposed or imprisonment for a term not exceeding two years, or both. There are exemptions from the provisions of PDPA for personal data processed by an individual for that individual's personal, family or household affairs.

Exemptions[99]

Exemptions from the provisions of PDPA for personal data processing will be extended to individuals only for the purposes of their personal, family or household affairs and for recreational purposes. Exemptions are also extended if personal data is processed to:

- prevent or detect a crime or for law enforcement or judicial investigation
- apprehend or prosecute offenders
- assess or collect any tax or duty or any other imposition of a similar nature.

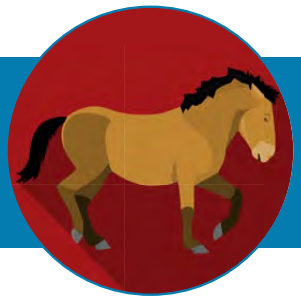
[97] https://www.thestar.com.my/news/nation/2019/09/23/malindo-says-data-breach-contained-source-identified-and-police-reports-lodged-in-malaysia-india
[98] https://tv.thethreatreport.com/cyber-security/data-breach-hits-malaysian-university-personal-data-leaked/
[99] Section 45, PDPA

Relevant laws, directives and terminology reference

Standard	Industry	Regulator	Applicability
Personal Data Protection Standard, 2015	All	Commissioner	Data users
Computer Crimes Act, 1997	All	Commissioner	
Communications and Multimedia Act, 1998 (CMA)	Telecom	MCMC	Network service providers
PDP Code of Practice – For Licensees Under the Communications and Multimedia Act, 1998	Network, Application, Content Application Providers	MCMC	Data users

Terminology	Definition
Data user	any person who processes and has control over, or authorises the processing of personal data within commercial transactions
COVID-19	Coronavirus Disease 2019

Mongolia



The laws pertaining to privacy and data protection in Mongolia are 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 protection for 'personal secrets', which are categorised as information such as correspondence, health, property, family and others prescribed by law. Disclosure of that information is generally prohibited except for national security purposes and to protect public health or legitimate interests. The Act defines and categorises the right to privacy as secrets of:

- correspondence
- health information
- property
- family
- other information, as and when defined by the laws of Mongolia.[100]

The Law of Mongolia Organisational Secrets, 1995 (the Organisation Privacy Law), is the primary law that regulates corporate data protection. It states that an organisation must protect the personal secrets of an individual it has acquired in the same manner that it protects its own secrets. Article 16.13 of the Constitution of Mongolia, enacted on 13 January 1992, provides that the personal, family, and correspondence privacy of a citizen must be protected by law. Article 16.17 of the Constitution provides that the safety of an entity's and individuals' secrets must be protected by law.[101]

The legal action against the violation of the 'privacy of correspondence' and 'disclosure of private secrets' is established in Articles 135 and 136 of the Criminal Code of Mongolia. Violations of privacy imply criminal, material or administrative legal liabilities.

Key considerations:

Open data: In 2013 Mongolia implemented an open government partnership initiative with the United States to increase transparency and reduce corruption in trade and commerce. This initiative was followed by an open data initiative in 2014 with the United States, which included open data projects across multiple government agencies. In September 2013 the United States and Mongolia signed the US-Mongolia Agreement on Transparency in Matters Related to International Trade and Investment, or Transparency Agreement (TA). Mongolia's Parliament ratified the TA in December 2014. The United States and Mongolia certified that their respective applicable legal requirements and procedures were completed in January 2017 and the TA entered into force 20 March 2017.[102]

[100] https://www.dataguidance.com/notes/mongolia-data-protection-overview
[101] https://www.dataguidance.com/notes/mongolia-data-protection-overview [1]https://www.dataguidance.com/notes/mongolia-data-protection-overview
[102] https://www.privacyshield.gov/article?id=Mongolia-Transparency-of-the-Regulatory-System

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' that require protection. This law restricts their use and disclosure with associated offences for breaches, indirectly creating an obligation for information security.

Cases

- **2018** - A group of hackers infiltrated a Mongolian government data centre to compromise government resources, including government websites.[103]

Relevant laws, directives and terminology reference

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
Constitution of Mongolia	All	The Mongolian Government	Everyone

[103] https://www.cfr.org/cyber-operations/compromise-mongolian-government-data-center

Myanmar

The Constitution under Section 357 of the Republic of the Union of Myanmar 2008 protects the privacy of home, property, correspondence and other communications of the citizens of Myanmar.[104] While Myanmar does not have specific privacy laws, the **Law Protecting the Privacy and Security of Citizens**, 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.

Key considerations:

Power of the government: The provisions under the Law Protecting the Privacy and Security of Citizens can be bypassed and circumvented with permission from the President or a government body. The Telecommunications Law empowers the Ministry of Communications and Information Technology (MCIT) to control and access information transmitted by telecommunication service providers and their equipment.

Biometric data collection: In December 2019, the Ministry of Transport and Communications developed a strategy to create a national database of private citizen information by making biometric data collection mandatory when purchasing mobile phone services.[105]

Supporting legislation

- The Electronic Transactions Law, 2004[106] (amended in 2014)
- The Competition Law, 2015.[107]

Use and disclosure

As per the Law Protecting the Privacy and Security of Citizens, no person shall:

- have their interpersonal communication or communications equipment intercepted or circumvented
- request or obtain personal telecommunications or any other electronic data from telecommunication operators

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

[104] http://www.myanmar-law-library.org/IMG/pdf/constitution_de_2008.pdf
[105] https://www.biometricupdate.com/201912/myanmar-to-introduce-mandatory-biometric-data-collection-for-massive-national-database
[106] https://www.myanmartradeportal.gov.mm/en/legal/216
[107] https://www.asean-competition.org/file/pdf_file/Myanmar-Competition%20Law%20(English%20Version).pdf

Regulators and regulatory landscape

The MOHA and the MCIT are the shared regulators of privacy and data protection within Myanmar and are responsible for the roles and responsibilities to protect the privacy and security of citizens, and receive and handle complaints.

Cases

- **2019** – A group of hackers called Cyber 72 attacked 20 Myanmar websites, eight of which were government websites. In this attack, four of the websites were defaced and others were hit with distributed denial-of-service attacks.[108]

Penalties

As per section 8 of the Law Protecting the Privacy and Security of Citizens, no-one shall:

- have their interpersonal communication intercepted or their equipment used for communication circumvented
- demand or obtain personal telephonic and electronic communications data from telecommunication operators
- open, search, seize or destroy another person's private correspondence, envelope, package or parcel.

In the case of a breach of Section 8 of the Law Protecting the Privacy and Security of Citizens, a six months to three years prison sentence may be mandated along with a fine range of K300,000 to K1,500,000.

Under the Electronic Law, 2004, per section 34, whoever commits any of the following acts shall, on conviction, be punished with imprisonment for a term which may extend to five years,[109] or with a fine, or with both when:

- sending, hacking, modifying, altering, destroying, stealing, or causing loss and damage to the electronic record, electronic data message, or the whole or part of the computer program
- intercepting any communication within the computer network
- using or giving access to any person of any fact in any communication without permission of the originator and the addressee
- communicating to any other person directly or indirectly the security number, password or electronic signature of any person without the permission or consent of such person
- creating, modifying or altering information or distributing information created, modified or altered by electronic technology to the detrimental interest of or to lower the dignity of any organisation or any person.

Under Competition Law 2015 Section 19 on disclosing secrets of another business[110] no business shall:

- infringe security measures to access and collect business secrets and information
- use or reveal business secrets without permission from the lawful owner of the secrets
- deceive a person obliged to maintain secrets or abuse their confidence by accessing, collecting, collecting or revealing business secrets or information related to such secrets
- leak economic information by infringing security measures adopted by public (government) companies
- leak business secrets and procedures of product distribution
- indulge in trade and commerce by leveraging leaked confidential information.

[108] https://elevenmyanmar.com/news/bangladesh-hackers-attack-ten-myanmar-websites
[109] https://www.myanmartradeportal.gov.mm/en/legal/216
[110] https://www.asean-competition.org/file/pdf_file/Myanmar-Competition%20Law%20(English%20Version).pdf

Relevant laws, directives and terminology reference

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

Terminology	Definition
Agency	any government ministry or department including educational institutions and statutory bodies
Data	information in electronic or manual form
Personal Information Controller	a person or organisation that controls or instructs another person or organisation to collect, hold, process, use, transfer or disclose personal information.

New Zealand

Privacy in New Zealand is regulated by the Privacy Act, 1993, which contains principles on how agencies - defined as any person, body of persons, or department, whether corporate or unincorporated, and whether in the public sector or the private sector - should collect, use, disclose, store, retain and provide access to personal information.

The Privacy Act 2020, which amends the Privacy Act 1993, received Royal Assent on 30 June 2020. The amendments come into effect on 1 December 2020 and provide better alignment with certain requirements in the EU's GDPR, notably the 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 the Privacy Act 2020.[111]

Primary legislation: Privacy Act, 1993 and Privacy Act 2020 (effective 1st December 2020)

Key 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 Winston Peters v Paula Bennett and others 2020.[112] The tort contains two elements which must be proven and have:

- a reasonable expectation of privacy in accordance with the facts of the case
- publicity, considered to be highly offensive to an objective, reasonable person with the burden of proof resting on the victim's ability to prove that 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 EU law. This means that personal data can be transferred from any of the 27 EU member states to New Zealand for processing without requiring any further safeguards. However, the EU will be re-evaluating New Zealand's adequacy status given the amendments made to the Privacy Act.

Unique identifiers: Unique identifiers, such as a customer driver's licence and passport numbers, must not be assigned to individuals unless necessary for an agency to carry out any of its functions efficiently. Agencies are also mandated to take all reasonable steps to minimise the risk of misuse of a unique identifier before disclosing it to another agency. This measure seeks to reduce identity theft by helping to control the publication of unique identifiers.

[111] http://legislation.govt.nz/bill/government/2018/0034/latest/LMS23223.html
[112] https://www.privacy.org.nz/blog/winston-peters-v-paula-bennett-and-others/

Guidelines for landlords and tenants: The Office of the Privacy Commissioner (OPC) has produced guidelines for landlords, outlining the information that should and should not be collected when deciding on an individual being suitable as tenant. For example, the collection of bank statements to determine an individual's ability to pay rent is permissible. However, collecting bank statements to determine spending habits is unfair and unreasonably intrusive.

Information sharing guidelines – child welfare and family violence: The Ministry of Justice and Oranga Tamariki (Ministry for Children) have each released new guidance on requesting, sharing, and using personal information. The intention is to propagate safe and appropriate information sharing, which will help ensure everyone working with tamariki (children) can collaborate in the best interests of the child.

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. This also applies to individuals whose death is maintained according 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. Agencies must take reasonable steps to notify individuals at the time of collection, or as soon as possible, as to:

- its occurrence
- its purpose
- the intended recipients
- the collector's and/or information holder's contact details
- any law requiring collection, and if so, whether voluntary or mandatory
- possible consequences if all or part of the information are not provided
- their rights to access and correct the information collected and held about them.
- right to refuse consent and any implications arising from refusal.

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 for which it was collected and must not disclose it 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.

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.

Data retention and destruction

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may be lawfully used.

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 variety 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 currently not mandatory. However, the OPC provides guidance on responding to a data breach as best practice.[113] Once introduced, the Privacy Act 2020 seeks to make the notification requirement mandatory.

[113] https://www.privacy.org.nz/privacy-for-agencies/data-breaches/

Voluntary guidance	
Threshold for reporting	Reporting should occur where personal information has been inappropriately accessed, collected, used or disclosed considering the: • 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 be notified in the event of a data breach • Affected individuals should be notified directly to by phone, letter, email or in person • If direct notification could cause further harm, indirect notification should be made through websites, notices or media.
Content	Notification must 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 the OPC, enquiries and complaints • appropriate support when necessary e.g. advice on changing passwords.

The Privacy Act 2020:
The Privacy Act 2020 requires agencies to **mandatorily inform** the Privacy Commissioner and affected individuals when a privacy breach causes harm or poses a risk of harm to people. Not notifying the Commissioner would be an offence.[114]

The Privacy Act 2020 defines a **privacy breach** in relation to personal information held by an agency as an unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information, or an action that prevents the agency from accessing the information on either a temporary or permanent basis.

A **notifiable privacy breach** has been defined as a privacy breach that can reasonably be believed to have caused serious harm to affected individuals, or is likely to do so, but does not include a breach of the personal information held by an agency that is an individual, and that the information is held solely for the purposes of, or in connection with, the individual's personal or domestic affairs.

Breaches should **only be notifiable if they cause serious harm**. Agencies are mandated to notify the Commissioner as soon as practical after becoming aware of a notifiable privacy breach. Agencies would also be mandated to notify the affected person. A notifiable privacy breach means a breach that has harmed, or poses a risk of harm, to an individual.

Domestic or personally held information would be **exempt**. Individuals would not have to notify privacy breaches where the information is held solely for the purposes of, or in connection with, their household or personal affairs.[115]

The Office of the Privacy Commissioner is seeking expressions of interest from **commercial practitioners** with a strong emphasis on privacy and data protection, to develop model contractual privacy clauses.

[114] https://privacy.org.nz/privacy-for-agencies/privacy-breaches/responding-to-privacy-breaches/
[115] http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297421.html

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 the protections within or comparable to the Privacy Act
- transfer would be likely to contravene the basic principles set out by the OECD with regards to the security and use of personal information.

The Privacy Act 2020

- **Model contractual clauses:** The OPC is currently seeking consultation from commercial practitioners in privacy and data protection to develop model contractual clauses for facilitating cross-border disclosures. The use of model clauses would be an option for an agency to demonstrate compliance with the new Information Privacy Principle (IPP) 12 in clause 19 of the Privacy Act 2020. The obligations require the recipient of personal information to protect the information in comparable way to the safeguards in the Privacy Act 2020.
- **Privacy principle 12:** A new privacy principle proposing a series of controls on disclosing personal information to foreign agencies or persons. The principle proposes that an agency disclosing personal information to foreign persons or entities may only make that disclosure if it reasonably believes the foreign person or entity is meeting at least one of the following:
  - carrying on business in New Zealand and is subject to the Privacy Act 2020
  - subject to privacy laws that overall, provide comparable safeguards required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act 2020 (for example, by agreement between the agencies)
  - subject to the privacy laws of a country, province or State, or is a participant in a binding scheme for international disclosures of personal information, prescribed in regulations by the New Zealand Government as providing comparable safeguards to the Privacy Act 2020.
- **Cloud storage providers:** The principle provides that sending information to another organisation to hold or process on your behalf (as your agent) will not be not treated as a disclosure under the Privacy Act 2020, including an agency providing cloud storage services on behalf of the NZ based client. However, the principal organisation will be responsible for ensuring that the agent handles the personal information according to the provisions of the Privacy Act 2020.
- **Individual authorisation:** The principle mandates an agency wanting to rely on individual authorisation, must expressly inform the individual that the foreign entity or person may not be required to protect the information in a way that, overall, provides comparable safeguards. Additionally, the principle also enables disclosure of personal information overseas if it is necessary to avoid prejudice to the maintenance of the law (including the prevention, detection, investigation, prosecution and punishment of offences), or to prevent or lessen a serious threat to public health or safety or the life or health of an individual.

Codes of practice

The Privacy Act, 1993, gives the Privacy Commissioner the power to issue codes of practice that become part of the law. These codes may modify the operation of the Act for specific industries, agencies, activities or types of personal information. Codes often modify one or more of the information privacy principles to take account of special circumstances which affect a class of agencies (e.g. credit reporters) or a class of information (e.g. health information). Codes of practice are a flexible means of regulation and can be amended or revoked by the Privacy Commissioner at any time.

The following codes are currently in place:

- Civil Defence National Emergencies (Information Sharing) Code
- Credit Reporting Privacy Code
- Health Information Privacy Code
- Justice Sector Unique Identifier Code
- Superannuation Schemes Unique Identifier Code
- Telecommunications Information Privacy Code

Governance

Agencies are required to appoint a privacy officer.[114] The privacy officer is responsible for:

- encouraging compliance with the Privacy Act 2020
- dealing with requests made to the agency, such as access and correction
- working with the Commissioner in relation to investigations.

Regulators and regulatory landscape

The OPC 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.

Exemptions[117]

Organisations that aren't covered by the Privacy Act include:

- **Members of Parliament** (MPs), when they are acting as MPs. It is up to the Parliament or political parties to discipline MPs for breaches of privacy
- **Courts and tribunals**, in relation to their judicial functions. You have to challenge judicial decisions through the normal processes, such as an appeal
- **The news media** when they are conducting their news activities. The Media Council and the courts govern the news media
- **Individuals** who collect or hold personal information for their own personal, family or household affairs are exempt. This exemption does not apply if that collection, disclosure, or use of information would be highly offensive to an ordinary reasonable person
- **In special circumstances** the Commissioner can authorise agencies to collect, use or disclose information even when that would usually breach principles 2 (source of personal information), 10 (limits on use of personal information) and/or 11 (limits on disclosure of personal information).

[116] http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297074.html
[117] https://privacy.org.nz/further-resources/knowledge-base/view/101?t=224760_309556

Penalties

The Privacy Act 1993
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 NZ$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 for a privacy matter to date is NZ$168,000.

The Privacy Act 2020
The privacy bill would create new criminal offences, including:

- misleading an agency to obtain access to someone else's personal information
- destroying a document containing personal information, knowing that a request has been made for it.[118]

Fines for offences would be NZ$10,000 except in the case of class action law suits wherein the maximum award will be NZ$350,000 for each member of the class action.

Cases

- **2020 –** A public sector organisation in New Zealand reported a security incident impacting around 26,000 customers in February 2020. The incident had occurred between December 29, 2019, and January 27, 2020. The data leaked in the incident included full names, addresses, tax identification numbers, and photo identification such as passports or driver's licenses.[119]
- **August 2019 –** Nearly a million people faced the risk that their medical data had been accessed illegally after a website cyber-attack. The health firm's website was hacked in August, but investigations also uncovered previous attacks dating from 2016 to March 2019. The health firm, collects and analyses patient information from medical centres.[120]
- **June 2019 -** A government ministry was the victim of more than 180 million hacking attempts in less than 18 months. Three government departments confirmed they had been targeted by hackers and many more revealed they were under constant cyber-attacks. One prominent government agency said that between early 2017 and May last year, it was hacked three times and malware was introduced to its systems.[121]

[118] http://legislation.govt.nz/bill/government/2018/0034/latest/whole.html#LMS23223
[119] https://portswigger.net/daily-swig/generate-data-breach-impacts-26-000-new-zealand-residents
[120] https://in.reuters.com/article/us-newzealand-cyber/medical-data-breach-puts-details-of-a-million-new-zealanders-at-risk-idINKBN1WK03D
[121] https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12244938

Relevant laws, directives and terminology reference

Law/Decree	Industry	Responsible ministry	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 (PNG) does not have privacy legislation. However, the Cybercrime Code Act 2016 helps to regulate activities, crimes and offences conducted through electronic systems and devices, or information and communication technologies. Examples of such offences include illegal interception, unauthorised access or hacking and data interference.

The Constitution of the Independent State of Papua New Guinea provides the express right to reasonable privacy.[122] This right is upheld by the National Information and Communications Tech Act 2000 which, with the Protection of Privacy Communications Act 1973, helps ensure prevention against:

- interception, modification or recording of any communications by Information Communications Technology (ICT) service people
- damaging or tampering with network services
- obstruction of the transmission or delivery of communications sent via an ICT service
- infringement of personal privacy by an individual of another.

Key considerations:

Right to freedom of information:[123] Section 51 of the Constitution provides citizens the freedom of information to gain the 'right of reasonable access to official documents' subject to exceptions including national security, defence, international relations and the maintenance of personal privacy and security of the person.

Definition of personal information

Personal information has not been defined. However, 'data' is defined to include any representation of facts, concepts, information that is either text, audio, video, audio-visual or images or 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.

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 subject of such information or personal data
- classified or intended for restricted use or specified persons only
- related to the State, politics and the military, corporate secrets, or otherwise unavailable to the public.

[122] https://wipolex.wipo.int/en/text/199188
[123] https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/44016/70625/F868019216/PNG44016.pdf

2020 – YuTru is PNGs first private-sector led scheme for digital identification to enable citizens to engage in the online economy.[124] It will be used online and via mobile networks based on international best practices for computer security and cryptography. YuTru is based on a rules-based legal framework which takes into account privacy and security and is expected to launch 1 January 2021 with support and consultation provided by various banks and the Australian government's Department of Foreign Affairs and Trade.[125]

Relevant laws, directives and terminology reference

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

[124] https://www.businessadvantagepng.com/five-questions-for-yutrus-tony-willenberg/
[125] https://yutru.org/?page_id=101

The Philippines

In the Philippines, privacy and data protection are governed by the Data Privacy Act of 2012 (DPA),[126] which provides comprehensive protection for personal information. It is supported by the Implementing Rules and Regulations of the Data Privacy Act of 2012.[127] With a rapidly growing IT infrastructure, digital economy and population of social media users, the government and its privacy regulator have a mandate to protect the privacy of individuals while enabling the free flow of information.

In order to update and improve the DPA, there are currently two bills pending in the House of Representatives.[128] The first of these is House Bill No. 1188, which seeks to impose stiffer penalties for violations of the law. The second bill is House Bill No. 5612, which covers a wide range of topics including amendments to the definition of sensitive personal information, extra territorial application, Data Privacy Principles, the legal basis for processing sensitive personal information, data subject rights pertaining to reasonable access and data portability and the personal information processor's obligation to notify the National Privacy Commission (NPC) in the event of a data breach.

Primary legislation: Data Privacy Act of 2012 (the Act)

Key considerations:

Registration of data processing activities:[129] The DPA requires organisations, personal information controllers (PIC) and/or personal information processors (PIP) covered by the registration requirement[130] to maintain records of their data processing systems and register them with the NPC.

Extraterritorial jurisdiction: The Act applies to processing personal information belonging to Philippine citizens in and outside the Philippines, to organisations based in, carrying out business in, or processing personal information collected or held by an entity in the Philippines.

Distinction 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.

[126] https://www.privacy.gov.ph/data-privacy-act/
[127] https://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/
[128] http://ateneo.edu/udpo/article/amending-the-data-privacy-act
[129] https://www.privacy.gov.ph/npc-circular-17-01-registration-data-processing-notifications-regarding-automated-decision-making/
[130] https://www.privacy.gov.ph/wp-content/uploads/2017/08/NPC17-01_Appendix-1.pdf

Provisions specific to government: The Act imposes specific requirements for government entities on transmitting data to third parties and additional penalties on government officials who breach the Act while carrying out their duties.

E-commerce guidelines: The insurance e-commerce guidelines cover electronic privacy issues, particularly direct marketing and the use of cookies. It is mandatory to include a privacy policy on an organisation's website and to include details on the use of cookies. It also provides guidelines on direct marketing by e-mail to individual subscribers.

Definition of personal information

Personal information is defined as any information, whether in material form or not, from which an individual can be identified by the entity holding the information, or when combined 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, colour, and religious, philosophical or political affiliations, health, education, genetic or the sexuality of a person, or any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings. Sensitive information also includes any information issued by government agencies that are particular to an individual and include, but are not limited to, social security numbers, previous or current health records, licenses or their denial, suspension or revocation, tax returns and any classified information specifically established by an executive order or an act of Congress.

Collection and notice

When collecting personal information data must be:

- collected only for a specific, declared and legitimate purpose
- accurate, relevant and up to date where necessary
- adequate and not excessive in relation to its purpose
- deidentified 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
- scope and method of processing
- recipients or classes of recipients to whom the personal data will be disclosed
- methods of accessing the data
- identity and contact details of the data controller
- period for which the data will be stored
- rights the data subject may have.

Data subjects need to be notified and given an opportunity to withhold consent if any changes to their original, consented information is proposed.

Use and disclosure

Personal information must be accurate and relevant. It must be processed fairly and lawfully, and in a manner that is compatible with its declared purpose and ensures appropriate privacy and security safeguards. Processing personal data must 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
- to meet the legitimate interests of the controller or third parties that legally 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 where an adequate level of protection is ensured
- for the protection of lawful rights and interests of individuals.

Consent to processing 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 of securely and so as to prevent further processing, unauthorised access or sharing with 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.

Individual rights

The data subject is entitled to:

- **be informed** that their personal information is being processed, the processing's purpose, scope and method, the retention period, information recipients, identity of the controller, date the data was last accessed or modified and of their rights
- **access their personal information** and from where the data was collected, the names and addresses of recipients, manners of processing, reasons for disclosure and information about automated data processing where the data is likely be the sole basis for a decision affecting the data subject
- **request deletion or suspension of processing** where the data subject has established that their information is incomplete, inaccurate, outdated, falsely or unlawfully obtained, is being used for unauthorised purposes, is no longer necessary for the declared purposes, or where they withdraw consent or object to the processing
- **be indemnified for any damage** sustained due to their personal information having been inaccurate, incomplete, outdated, false, unlawfully obtained or subject to unauthorised use

- **data portability** giving the right to obtain a copy of their personal data in an electronic or structured form to allow for further use.

Individual rights do not apply where personal information is used only for scientific and statistical research, provided that their information is not used to determine decisions regarding the data subject. The lawful heirs and assignees of the data subject may invoke the rights of the data subject for which he or she is an heir, or assignee at any time after the death of the data subject, or when the data subject is incapacitated, or incapable of exercising their rights.

Data breach notification

It is mandatory to notify the NPC and data subjects in the event of a data breach of personal information. The NPC may exempt a controller from notification if it is in the public interest. It may also authorise postponing notification if it hinders the progress of a criminal investigation relating to a serious breach. All data breaches need to be documented in written reports and include the facts of the incident, effects of the incident and the remedial actions taken by the controller to respond to the breach.

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 danger. They should ensure the appropriate safeguards are implemented to protect their computer networks, including:

- a security policy on processing personal information
- identifying and assessing reasonably foreseeable vulnerabilities in their networks
- taking corrective mitigating actions against security incidents that can lead to a breach
- regularly monitoring 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.

Voluntary guidance

Threshold for reporting	Controllers must notify the NPC and affected data subjects when sensitive information or other information likely to enable identity fraud is: • 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 and affected data subjects.
Content	• nature of the breach, chronology of events, and an estimate of persons affected[131] • 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.

[131] https://www.privacy.gov.ph/memorandum-circulars/npc-circular-16-03-personal-data-breach-management/

Cross-border data transfer

Private sector
Before sharing data, controllers must obtain consent from the data subject and provide details of the transfer that includes relevant data, the recipients and the data subject's rights. Consent is required even when the data will 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 is subject to review by the Commission, on its own initiative or on complaint of a data subject.

Public sector
Data-sharing between government agencies for a public function or service is covered by a data-sharing agreement guaranteeing compliance with the Act, including safeguards for data privacy and security. The data-sharing agreement is subject to review by the Commission, on its own initiative or on complaint of a 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 controller or processor and any designated DPO remains accountable and must oversee the performance of the outsourced DPO.

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 ₱2,000,000, or a term of imprisonment between one to three years, and ₱4,000,000, or a term of imprisonment between three to six years for the unauthorised processing of sensitive information.

Registration of data processing activities

Personal information controllers and/or personal information processors are obliged to register their data processing systems with the NPC if they qualify through the:

- organisation employing at least 250 employees
- processing activity including sensitive personal information of at least 1,000 individuals[132]
- processing being likely to impose a risk to the rights and freedom of data subjects
- processing considered 'non-occasional' such as recurring high volume processing activities conducted by banks, universities and hospitals etc.

Data processing systems that involve automated decision-making must, in all instances, be registered with the NPC.

Regulators and regulatory landscape

The 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.

Cases

- **April 2019 -** An airline company reported a data breach of its rewards platform.[133] It experienced unauthorised access to the rewards platform server and had to shut it down temporarily. The airline confirmed that no credit card information was stored on its rewards platform. The DPO of the airline emailed a preliminary notification of the breach to the NPC.
- **October 2019** - The NPC imposed a ban on the processing of personal data by 26 online lending operators.[134] The operators used personal data of users' mobile contact lists to contact third parties and disclose personal data without users' consent. They also used this data to shame the borrowers into settling their loans.

[132] https://www.privacy.gov.ph/wp-content/uploads/2017/08/NPC17-01_Appendix-1.pdf
[133] https://iapp.org/news/a/cebu-pacific-confirms-data-breach/
[134] https://iapp.org/news/a/alleged-privacy-breach-leads-to-npc-summons-for-online-lenders/

Relevant laws, directives and terminology reference

Law/Decree	Industry	Responsible ministry	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	Definition
Data subject	an individual whose personal, sensitive personal, or privileged information is processed
Personal information controller	a person or organisation that 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 their behalf This excludes a person or organisation following instructions of another person or organisation and individuals who collect, hold, process or use personal information in connection with the individual's personal, family or household affairs
Personal information processor	any natural or judicial person to whom a personal information controller outsources processing the data subject's personal data
The rules	implementing rules and regulations of the Data Privacy Act of 2012
Consent	freely given, specific and informed indication of will
COVID-19	Coronavirus disease 2019

Singapore

Singapore's privacy framework is governed by the Personal Data Protection Act 2012 (PDPA), supported by additional regulations, including the Personal Data Protection (Enforcement) Regulations and Personal Data Protection Regulations. The Singapore government is currently reviewing its current privacy framework and is expected to make amendments to the law and introduce a mandatory data breach notification requirement. In May 2020, the Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PDPC) jointly initiated an online public consultation on the proposed amendments to the PDPA.[135]

Primary legislation: Personal Data Protection Act 2012 (PDPA)

Key considerations:

Key highlights of amendments proposed to PDPA:[136]

- **Mandatory data breach notification:** Organisations will be required to notify the PDPC of a data breach that results in, or is likely to result in, 'significant harm' to the individuals affected by the breach, or is of a 'significant scale'. Significant scale could indicate a systemic issue within the organisation and may require further investigation and guidance from the PDPC on implementing appropriate remedial action. Organisations will be required to notify the affected individuals if the data breach is likely to result in significant harm to them. The types of personal data covered could include national identification numbers, health records, financial information and criminal records.
- **Meaningful consent:** The concept of 'deemed consent' will be expanded to include meaningful consent in order to facilitate using and processing personal data for reasonable business purposes and will cover circumstances where:
  - collecting, using or disclosing personal data is reasonably necessary to perform or conclude a contract or transaction
  - individuals are notified of the purpose of the intended collection, use or disclosure of their personal data, and are given a reasonable opportunity to opt-out, and have not opted out.
- **Consumer autonomy:**
  - **Data portability:** To enable easier switching, the new data portability obligation allows consumers to request a copy of their personal data be transmitted to another organisation. With access to more data the new obligation will support the development of new services and applications.
  - **Expanded protection from unsolicited messages:** Sending unsolicited messages to telephone numbers through the use of dictionary attacks and address harvesting software will be prohibited under the PDPA's 'Do Not Call' provisions. The Spam Control Act (SCA) will also be amended to cover commercial text messages sent in bulk to instant messaging accounts.

[135] https://www.pdpc.gov.sg/news-and-events/press-room/2020/05/mci-and-pcpc-launch-online-public-consultation-on-personal-data-protection-(amendment)-bill-2020
[136] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Press-Room/2020/Media-Release---Launch-of-Public-Consult-of-PDP-(Amendment)-Bill-2020---14-May-2020.pdf?la=en

- **Effectiveness of PDPC's enforcement:** The PDPC will strengthen its enforcement powers as a deterrent, increasing financial penalties for organisations that breach the PDPA up to 10% of their annual turnover or S$1 million, whichever is higher.

Data protection in the public sector: Personal data protection in the public sector is governed by the Public Sector (Governance) Act 2018 and supported by the Government Instructions Manual. Broadly aligned to the PDPA[137] the legislation is separate to that governing the private sector.

National Registration Identity Card (NRIC) numbers: The PDPC released guidelines on the PDPA's application to NRIC and other national identification numbers with effect from 1 September 2019. The guidelines state that national identification numbers can only be collected and retained if required under the law and necessary if a high degree of fidelity is required to verify the identity of the individual.[138]

AI framework: In January 2020, the PDPC released the second edition of its Model AI Governance Framework for consultation, adoption and feedback. The Model Framework provides detailed and readily implementable guidance to private sector organisations to address key ethical and governance issues and be mindful of privacy obligations mandated by the PDPA when deploying AI solutions.[139]

Cross-border transfers: In June 2020, the PDPC amended the Personal Data Protection Regulations to recognise the Asia Pacific Economic Cooperation's Cross Border Privacy Rules and associated Privacy Recognition for Processors certification system for transferring data overseas. The amendment ensures that organisations in Singapore can transfer personal data to the approved overseas recipient without meeting additional requirements. Singapore has also developed a model sample contract clause that transferring organisations can include in their contract with recipients.[140]

[137] https://sso.agc.gov.sg/Acts-Supp/5-2018/Published/20180305?DocDate=20180305#:~:text=7%20February%202018.&text=An%20Act%20to%20provide%20for,amendments%20to%20certain%20other%20Acts.
[138] https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-nric-and-other-national-identification-numbers#:~:text=Advisory%20Guidelines%20on%20the%20Personal%20Data%20Protection%20Act%20for%20NRIC,of%20physical%20NRICs%20by%20organisations.
[139] https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework
[140] https://www.pdpc.gov.sg/news-and-events/announcements/2020/06/singapore-now-recognises-apec-cbpr-and-prp-certifications-under-pdpa

Definition of personal data

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 access
- whether the data is true or not.

The PDPA does not apply to:

- personal data in a record that has existed 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 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 is disclosed to another organisation.

Use and disclosure

Personal data can only be used and disclosed according to its original collection purpose and where a reasonable person would consider the purpose appropriate in the circumstances. The individual must provide consent for any use and disclosure. An individual may be deemed to have consented for a purpose if they have voluntarily provided personal data for that purpose and it is reasonable that the 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, it 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 before 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 itself 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 message's recipient was or is present in Singapore when the message was accessed. The Spam Control Act (SCA) regulates electronic marketing activities. This includes sending unsolicited commercial communications in bulk, using electronic mail, SMS or MMS.

Data retention and destruction

An organisation must not retain personal data, and ensure steps are taken to deidentify the data as soon as it is reasonably assumed that the data no longer serves the purpose for which it was collected, or for any business or legal purpose. Although the PDPA does not prescribe a specific retention period of personal data, there may be specific industry-standard requirements that apply.

Security

An organisation must protect personal data in its possession or control, with adequate and reasonable security arrangements to prevent unauthorised access, collection, use, disclosure or similar risks. However, the PDPA is not prescriptive as to the particular security measures 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
- request as soon as reasonably possible, an organisation provide access to their information, including details as to how the information is used or disclosed
- request their personal information be corrected including any error or omission in their data, where it is in the possession or control of the organisation, and without being charged a fee for the correction. If the organisation is unable to correct the personal data within 30 days, the individual should be informed within 30 days.

Data breach notification

Requirements	
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 practical 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 third parties affected, e.g. banks, credit card companies, police.
Content	To include the: • extent of the data breach • type of personal data affected • amount of personal data affected • cause or suspected cause of the data breach • steps taken by the organisation to manage the risk and rectify the breach • information as to whether individuals have been notified • further steps to be taken by the organisation • contact for affected persons or the PDPC to access for further information.

Cross-border data transfer

Cross-border data transfer is allowed if the offshore third party has privacy protections comparable to Singapore 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.

Singapore recognises the APEC CBPR and PRP certifications for overseas transfers of personal data under the PDPA. Therefore, organisations in Singapore can easily transfer personal data to the overseas certified recipient without any additional requirements prescribed under the PDPA.

Regulators and regulatory landscape

The PDPC has the power to:

- prohibit the collection, use or disclosure of personal data that breaches any provision of the PDPA
- destroy personal data that has been collected in breach of the provisions of the PDPA
- refuse the right to access or correct personal data
- enforce financial penalties not exceeding S$1 million.

Exemptions

The PDPC may, with the approval of the MCI, exempt any person or organisation or any class of thereof, from all or any of the provisions of the PDPA.[141] On written application, the Commission may exempt any organisation wishing to transfer personal data to a country or territory outside Singapore from any requirement applicable for cross-border transfers including the need to be published in the Gazette. This exemption may be revoked at any time by the Commission.[142]

Cases

- **January 2019 -** Hackers stole the sensitive health records of 1.5 million SingHealth hospital patients and 160,000 outpatient prescription records. A financial penalty of S$250,000 was imposed on SingHealth for failing to make reasonable security arrangements to protect the personal data.[143]
- **March 2020** - The SSA Group International Pte Ltd was found to have breached its obligations to protect the personal data in its possession. A warning was issued by the PDPC to the SSA Group for failing to put in place reasonable security arrangements to prevent the unauthorised access of 53 individuals' course registration information that was publicly available on its webpage.[144]
- **February 2020 -** A financial penalty of S$16,000 was imposed on Royal Caribbean Cruises (Asia) for failing to put in place reasonable security arrangements to protect the personal data of its customers after some of that data was subject to a ransomware attack.[145]
- **March 2020 -** MCST 3593 and New-E Security failed to put in place reasonable security arrangements to prevent the unauthorised disclosure of CCTV footage of a common property at Marina Bay Residences. MCST3593 also failed to appoint a data protection officer or the policies and practices necessary for the organisation to comply with the PDPA.[146]

[141] Section 62 of PDPA
[142] Section 26 of PDPA
[143] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf
[144] https://www.pdpc.gov.sg/all-commissions-decisions/2020/03/breach-of-the-protection-obligation-by-ssa-group-international
[145] https://www.pdpc.gov.sg/all-commissions-decisions/2020/02/breach-of-the-protection-obligation-by-royal-caribbean-cruises-(asia)
[146] https://www.pdpc.gov.sg/all-commissions-decisions/2020/03/breach-of-the-protection-and-accountability-obligations-by-mcst-3593-and-breach-of-the-protection-obligation-by-new-e-security

Penalties

Offence	Applicability	Penalties	Imprisonment
Organisational breach any data protection provisions in the PDPA	Organisation/data users	Up to S$1 million	
Breach of DNC provisions	Individuals	Up to S$10,000 for each offence	Up to 12 months
DPO – non co-operative	Individuals	Up to S$10,000	Up to 12 months
DPO – non co-operative	Organisation	S$100,000	N/A

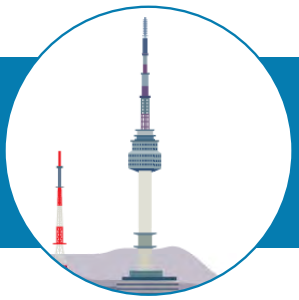
Relevant laws, directives and terminology reference

Standard	Industry	Regulator	Applicability
Computer Misuse Act	Comprehensive, refers to all individuals, regardless of nationality and citizenship, outside & within Singapore	Commissioner of police	Individuals and organisations
Cybersecurity Act	Applies to 11 vital sectors, including energy, health care, financial services and information communications	Cybersecurity commissioner	Critical information infrastructure organisations and data users
Personal Data Protection (composition of offences) Regulations, 2013	Comprehensive	Personal data protection commissioner	Organisations and data users
Personal Data Protection (DNC registry) Regulations, 2013	Comprehensive	Personal data protection commissioner	Organisations and data users
Personal Data Protection (enforcement) Regulations, 2014	Comprehensive	Personal data protection commissioner	Organisations and data users

Standard	Industry	Regulator	Applicability
Personal Data Protection Regulations, 2014	Comprehensive	Personal data protection commissioner	Organisations and data users
Personal Data Protection (appeal) Regulations, 2015	Comprehensive	Personal data protection commissioner	Organisations and data users
Public Sector (governance) Act, 2018	Public sector	Minister for Communications and Information	Public sector agencies

Terminology	Definition
Individuals	natural person, whether living or deceased
Organisation	any individual, company, association or body of persons, corporate or unincorporated, regardless of whether or not they: • formed or are recognised under the law of Singapore • reside, or have an office or a place of business, in Singapore.
SMS	Short Message Service
MMS	Multimedia Messaging Service

South Korea



South Korea's privacy frameworks contain 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.

Primary legislation: Personal Information Protection Act, 2011

Key considerations:

Amendments:[147] On 9 January 2020, the National Assembly of the Republic of Korea announced it had passed proposed amendments to the PIPA, known collectively as the Data 3 Act, the Act on Promotion of Information and Communications Network Utilization and Information Protection, 2001 (ICNA), and the Credit Information Use and Protection Act 2008. Through these amendments, duplicated articles in the ICNA and the Credit Act will be deleted and integrated into the PIPA. The regulatory body governing privacy protection of online services will be changed to the Personal Information Protection Commission (PIPC) from Korean Communications Commission (KCC). The amendments came into effect on 5 August 2020.

The amendments to PIPA include but are not be limited to:

- distinguished concepts of personal data, pseudonymised data and anonymised data (excluding anonymised data from the scope of personal data)
- defined permissible scope of pseudonymised data processing
- permitted processing of pseudonymised data for statistical, scientific research, or public interest record-keeping purposes
- permitted combinations of pseudonymised data of personal data controllers through specialised agencies
- imposed restrictions on pseudonymised data processing
- permitted use and release of personal data without obtaining data subjects' consent to an extent reasonably related to the original purpose of data collection
- elevated and strengthened Personal Data Protection Commission (PDPC)'s status and powers
- special provisions related to the deleted provisions of the previous ICNA.

[147] http://www.pipc.go.kr/cmt/main/english.do#

Embracing technology: South Korea is embracing and developing technology including big data, artificial intelligence, autonomous objects, virtual and augmented realities, IoT and robotics.

Global influences:[148] South Korea aims to align its privacy framework to global standards by seeking adequacy status from the European Commission to be able to freely transfer information between South Korea and the European Union.[149]

APEC: In 2017, South Korea became part of the Asia-Pacific Economic Cooperation (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 include a person's name, image and resident registration number. Information will be considered personal if it can be combined with other information to identify the individual, or, if not identifiable on its own, can be easily combined with other information to identify a specific individual. Factors to consider when combining include the feasibility of obtaining the other information, and the time, expense and technology needed.

Sensitive data includes information that is or is related to an ideology, belief, membership of a trade union or political party, political mindset, health and sexuality. 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 the data subject and make it available for public access. When obtaining consent, data subjects must be explicitly given notice, including where modified, of the:

- purpose and use for collection
- type of information collected
- period for use and retention
- right to refuse consent and any implications arising from refusal.

[148] https://www.dataguidance.com/opinion/south-korea-long-road-adequacy
[149] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

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, except where it is:

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

Provided the personal information is unidentifiable and consent was provided, it must:

- 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 law and regulation
- 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, it must store and manage that particular information separate from other personal information. It must also 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 including:

- 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

Processors must adhere to breach notification as provided by the PIPA.

Requirements	
Threshold for reporting	• When the personal information controller becomes aware of any personal information leak, it must immediately notify the affected data subject in writing. • The personal information controller is obliged to notify the data subject as soon as it has taken measures to prevent any dissemination of the leaked data or any additional leakage, including shutting down the access route, initiating check-up of weak points and deleting the leaked personal data. • If there is a large scale data breach, the personal information controller must report the breach to the PIPC or the Korea Internet & Security Agency (KISA) without delay, as well as the results of its preventative measures. • Where the personal information of more than 10,000 data subjects is leaked, the personal information controller is obliged to post the information on the security incident/breach, on its website for more than seven days.
Time frame	Processors must provide notification without delay.
Who to notify	• PIPC • KISA • Aggrieved data subjects
Content	Notification must include: • the kind of information leaked • when and how the information was leaked • remedies the data subjects can take to minimise further damage • countermeasures and remedial procedures to be taken by the processor • details of contact points, such as a help desk, to report damage.

Cross-border data transfer

Personal information can only be shared with third parties 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.

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

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.

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.

Exemptions

Provisions pertaining to processing and safeguarding personal information, data subject rights, dispute mediation committees and data protection collective suits shall not be applicable to personal information:

- collected by the Statistics Act among personal information processed by the public institutions
- requested to be provided for analysis relating to national security
- processed temporarily where urgently necessary for public safety and welfare, public health, etc.
- used for the internal reporting purposes of the press, missionary activities by religious organisations, and the nomination of candidates by political parties, respectively.

Provisions pertaining to collecting and using personal information, and any consent, limitations on transfer, data breach notification and processing suspension, shall not be applied when the personal information is processed by visual data processing devices installed and operated at open places. The said devices may only be installed if permitted by law and regulations and if necessary to:

- prevent and investigate crimes
- secure the facilities safety and prevent fire
- regulate and control traffic
- collect, analyse and provide traffic information.

Provisions pertaining to the collection and use of personal information, establishment and disclosure of privacy policy and designation of a privacy officer shall not apply to personal information processed by a personal information controller of groups or associations for friendship such as alumni associations and hobby clubs.

Cases

- **2019 –** South Korea was the victim of the largest Card Present (CP) data theft in the entire Asia Pacific region. Around 42,000 compromised South Korean-based CP records were posted for sale on the dark web.[150]
- **January 2020 –** the Seoul Eastern District Court found a travel agency guilty of negligence in failing to prevent a 2017 data breach that affected more than 465,000 customers of the agency and 29,000 of its employees. The privacy officer was accused of violating South Korea's Personal Information Protection Act and the ICNA, which require the person responsible for the management of personal data to take necessary 'technological and managerial measures' to prevent data breaches and to notify the Korea Communication Commission of any data breach incidents within 24 hours. The Court imposed a penalty of ₩10 million against the privacy officer. This was in addition to separate fines of ₩327,250,000 imposed against the company by the Ministry of Interior and Safety.

Penalties

Breaches within the Act can attract fines of up to ₩100 million and imprisonment of up to 10 years from the Ministry, with other bodies, including the PIPC, undertaking enforcement. In addition, data subjects may claim compensation of up to ₩3 million for data breaches caused by intentional or negligent violation of information and communications services providers.

[150] https://www.cisomag.com/data-breach-exposed-one-million-payment-card-details-in-south-korea/

Relevant laws, directives and terminology reference

Law/Decree	Industry	Responsible ministry	Applicability
Act on the Development of Cloud Computing and Protection of its Users 2015	All	Ministry of Science and ICT	Commercial cloud computing service providers
Act on Promotion of Information and Communications Network Utilization and Information Protection 2001	Information and Communication	KCC, Ministry of Science and ICT	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	Information and Communication	KCC, Ministry of Science and ICT	Information and communications service providers
Enforcement Decree of the Personal Information Act (Presidential Decree No.28355)	All	Ministry of the Interior and Safety, PIPC	Data controllers and processors
Personal Information Protection Act 2011	All	Ministry of the Interior and Safety, PIPC	Data controllers and processors

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.

Sri Lanka

There is a growing need to protect personal information for individuals in Sri Lanka with an increasing population 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 to a right to privacy, the Telecommunications Minister has released Draft Data Protection Legislation, also referred to as the Personal Data Protection Act 2019 (PDPA).[151] The PDPA provides for measures to protect the personal data of individuals that is held by banks, telecom operators, hospitals and other personal data aggregating and processing entities. The legislators have proposed the PDPA be implemented in stages. The PDPA will come into effect within a period of three years from the date the Speaker of the Sri Lankan Parliament certifies it. Additionally, the Data Protection Authority is mandated to be established within 18 months from the date the Speaker certifies the PDPA.[152]

Key considerations:

Digital identities: A national digital identity scheme, incorporating electronic identity cards and passports, and primarily concerning biometric data, was launched in 2019 to enable citizens to transact securely online, help prevent identity fraud and other related scams. [153]

Internet and social media use: Currently, 34% of the population use the internet, i.e. 7.13 million people, of whom 6.2 million are active social media users. Greater governance is necessary as social media use increases. Blocking access to social media is not uncommon.[154]

Cybersecurity Bill: The Cybersecurity Bill was released in 2019 to prevent, mitigate and respond to cybersecurity threats and incidents and establish the Sri Lankan Cybersecurity Agency. [155]

[151] http://www.mdiit.gov.lk/index.php/en/what-we-diliver/downloads/acts/send/23-acts/78-data-protection-bill-2019-10-03-amended-final
[152] http://www.mdiit.gov.lk/index.php/en/digital-news/item/73-data-protection-legislation
[153] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Sri-Lanka.pdf
[154] https://datareportal.com/reports/digital-2020-sri-lanka#:~:text=There%20were%206.40%20million%20social,at%2030%25%20in%20January%202020.
[155] https://www.medianama.com/2019/06/223-sri-lankas-new-cyber-security-bill-is-ready-cyber-security-agency-designation-of-critical-information-infrastructure-and-more/

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 in electronic transactions
- implementing data protection policies for the future.

Cases

- **2019** – The Sri Lanka Computer Emergency Readiness Team (CERT) identified that a group of unknown intruders allegedly attacked numerous Sri Lankan websites including the Kuwait Embassy in Colombo, the Tea Research Institute in Talawakelle and the Rajarata University in Mihintale. The attackers allegedly targeted vulnerable websites with minimum cybersecurity measures.[156]

Other considerations

In 2015 Sri Lanka joined the Budapest Convention, an international legally binding treaty on Cybercrime. This involves dealing with offences against:

- confidentiality, integrity and Information and systems availability
- computer related offences
- content related offences
- infringements of copyright and related rights.

It also discusses adopting legislation which enables searching a computer system for data and collecting real time computer data.

[156] https://www.cisomag.com/several-websites-in-sri-lanka-attacked/

Relevant laws, directives and terminology reference

Law, regulation, guideline or standard	Coverage/ industry	Regulator	Applicability
Information and Communications Technology Act, No. 27 of 2003	Comprehensive	ICTA	ICTA
Electronic Transaction Act, 2006	Electronic Contracts and certification services	N/A	Originators and addressees
Computer Crimes Act, 2007	Cybercrimes	Minister in charge of Science and Technology	Data subjects
The Telecommunication Act, 1996	Telecommunication transmissions	Telecommunication Regulatory Commission of Sri Lanka	Telecommunications officers and operators
Right to Information Act, 2016	Comprehensive	Office of the Australian Information Commissioner	Credit Providers and Credit Reporting Bodies

Terminology	Definition
Addressee	the person intended by the originator to receive the communication
Operator	a person authorised by license to operate a telecommunication system
Originator	a person, by whom 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
Citizen	a body, whether incorporated or unincorporated
Data Protection Authority	the Authority shall be responsible for all matters relating to personal data protection in Sri Lanka and for the implementation of the provisions of the Draft Data Protection Legislation.

Taiwan

In Taiwan personal information is protected under the Personal Data Protection Act (PDPA)[157] and enforced by industry regulators and local government authorities. The legislation was enacted in 1995 and amended in 2010 and 2015. When drafted, the PDPA considered the European Data Protection Directive (Directive 95/46/EC). In 2018, Taiwan was admitted to APEC's Cross Border Privacy Rules system[158] which aims to 'build consumer, business and regulator trust in cross border flows of personal information',[159] making Taiwan only the seventh APEC member economy to do so, highlighting its increased focus on privacy.

Primary legislation: Personal Data Protection Act (PDPA)[162]

Key considerations:

Trends to consider for Taiwan include:

Increasing 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 are 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 an ongoing debate as to whether data subjects have the right to opt out of having their deidentified information used by organisations to perform analyses.

The EU's GDPR: The extraterritorial reach of the GDPR has significant ramifications for Taiwanese businesses given the continually expanding size of Taiwan's international trade. For example, trade with the US increased by 13.6% in the first 11 months of 2019[160] and Taiwan received EU exports worth €51.9 billion in 2018.[161] The biggest impact is likely in the technology industry, where organisations with markets in the EU will need to comply with the GDPR.

Establishing a Personal Data Protection Office: In 2018, the National Development Council established the Personal Data Protection Office. The focus of the office is to address GDPR issues and coordinate with the relevant authorities. It is also working towards obtaining an adequacy decision from the EU that deems Taiwan to have an adequate level of protection for the cross-border transfer of personal data between the EU and Taiwan. While the National Development Council awaits a favourable GDPR adequacy decision, it has embarked on amending the PDPA to support the Smart Government Action Plan (approved by the Executive Yuan on 6 June 2019) to improve data security and strengthen cybersecurity.

[157] https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021
[158] http://www.taipeitimes.com/News/biz/archives/2018/12/11/2003705872
[159] https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx
[160] https://amcham.com.tw/2019/12/taiwan-usa-trade-and-investment-networking-center-opens-in-taipei/
[161] https://eeas.europa.eu/sites/eeas/files/2019_eu-taiwan_relations_en.pdf
[162] https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021

Definition of personal information

Personal data is defined under the PDPA as:

- the name, date of birth, I.D. card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexuality, health examination, criminal record, contact information, financial conditions and social activities of a natural person
- any other information which may be used to identify a natural person, directly or indirectly.

The PDPA defines sensitive data as data including medical records, medical treatment, genetic information, sexuality, health examination and criminal records. They are not to be collected, processed or used except in defined circumstances as mentioned in the PDPA.

Collection and notice

Collection of data is defined as 'to collect personal information in any form and way' and should be:

- respectful of the rights and interests of the data subject
- bona fide
- reasonable and fair
- limited to the purpose of collection.

On collecting data, the organisation is required to inform data subjects of the:

- organisation's name
- purpose of data collection
- time, location, receiver and uses of the data
- data subject's rights
- consequences if he or she chooses not to provide their personal information.

Use and disclosure

Personal information must only be used by businesses in compliance with the specific purpose of collection and:

- accords with a law
- has a contract or a quasi-contract in place with the data subject
- was voluntarily provided by the data subject or the data was lawfully made public
- is used for research by an academic research institution or for the public interest as statistics by a government agency. However, the information must be deidentified
- consent has been obtained
- does not harm the rights and interests of the data subject.

Non-government agencies must comply with at least one of the following before processing information:

- be in accordance with a law
- have a contract or a quasi-contract in place with the data subject
- be voluntarily or lawfully made public
- be used for research by an academic research institution or for the public interest as statistics by a government agency. In this case individual data subjects must not be able to be identified
- ensure consent has been obtained
- not harm the rights and interests of the data subject.

Government agencies must comply with at least one of the following before processing information:

- consent must be obtained
- it must not harm the rights and interests of the data subject
- it is within the scope of the job function provided by laws and regulations.

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

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

Data retention and destruction

Data may be retained while the purpose of processing exists, or during the agreed term of use. The information can be retained after this time period if consent in writing is given, or it is necessary for the performance of a job or is legally required. To be considered necessary, one of the following must apply:

- the retention period by law or in contract has not expired
- deletion would injure the interests of the data subject
- other legitimate grounds.

Individual rights

A data subject shall be able to exercise the following rights with regards to their personal data and such rights shall not be waived or limited contactually in advance:

- make an inquiry to review his/her personal data and to make a complaint
- request a copy of his/her personal data
- supplement or correct his/her personal data
- demand the cessation of the collection, processing or use of his/her personal data
- erase his/her personal data.

Security

The PDPA requires that organisations are able to ensure the security of personal data, preventing it from being stolen, altered, damaged, destroyed, lost or disclosed. When considering their required security, organisations should consider:

- allocation of personnel and resources
- definition of scope of personal data
- mechanisms to evaluate risk and manage personal data
- mechanisms to prevent, notify and respond to data breaches
- internal procedures to collect, process and use data
- information security and personnel
- promotion of acknowledgement, education and training
- facility security
- information security audit
- records of use and evidence preservation
- security improvement and data maintenance.

Data breach notifications:

It is not mandatory to notify the regulator of a data breach. However, notification to data subjects is mandatory.

Guidance

Threshold for reporting	• If a data breach has occurred, the breach must be investigated and reported to the data subject. • The breach notification may be by mail, email, fax, text or in an advertisement. There is no requirement to inform any regulator of a data breach occurring under the PDPA. Note, that regulators may require notification separately. • The Financial Supervisory Commission requires organisations to notify it in case a breach may affect business operations or many customers. • The Ministry of Health and Welfare requires notifications if there is a breach related to biobanks. • The Ministry of the Interior and Economic Affairs also has notification requirements.
Time frame	After investigating of the incident there is no particular timeline provided for reporting the breach.
Who to notify	Affected data subjects. The regulator is not required to be notified.
Content	• the occurrence of a data breach • steps taken by the organisation or government agency to resolve the breach.

Data transfer

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

Governance

Data Protection Officer-like roles are not required under the PDPA. Government agencies are required to hire personnel to secure and maintain files, but are not required to hire specific privacy SMEs.

Cross-border data transfer

While cross-border transfer of data is permitted, certain restrictions are in place, including:

- biological specimens in a biobank may not be transferred outside Taiwan
- international transmission of biobank data must be approved by the Ministry of Health and Welfare
- the Financial Supervisory Commission's approval is required to outsource retail operations
- telecommunications providers cannot transfer data to China.

If one or more of the following exists when a non-government agency seeks to transmit personal information internationally, the government authority in charge of the industry concerned may impose restrictions on that transmission where:

- major national interests are involved
- an international treaty or agreement so stipulates
- the country receiving the personal data lacks proper regulations on the protection of personal data and the data subjects' rights and interests may consequently be harmed
- international transmission of personal information is made through an indirect method in which the provisions of PDPA may not be applicable.

Regulators and regulatory landscape

The Ministry of Justice is the interpreting agency of the Personal Information Protection Act. It does not work as a data protection authority. It plans Taiwan's legal framework for data protection and interprets the PDPA. The PDPA is enforced by government regulators and governments. The Financial Supervisory Commission (FSC) (for the financial services sector) is the sole regulator that publicly publishes decisions relating to data protection.

Cases

- **2020** - Taiwan's President's Office was allegedly hacked, and the minutes from internal meetings were sent to reporters. The Criminal Investigation Bureau (CIB) is currently investigating this incident.[163]
- **2019** -The CIB stated that 228 Taiwanese Booking.com customers had been victims of fraud after their personal data was accessed by hackers. The CIB estimates that these customers suffered NT$30 million in losses as a result and appealed to the public to select e-commerce sites with stronger security mechanisms.[164]
- **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 due to human error.[165]
- **October 2014** - The right to be forgotten: A plaintiff was awarded NT$26,000 for violations of the Taiwan Civil Code and PDPA against a large Taiwanese retailer following requests to be removed from a mailing list which did not occur. A further 52 emails were subsequently received.[166]
- **2017 -** The FSC investigated an insurance agency that mailed personal information to third parties unintentionally due to errors in the software used to send notices. A penalty of NT$50,000 was imposed on the organisation and responsible party for failing to report the breach in the required timeframe.[167, 168]

[163] https://focustaiwan.tw/politics/202005160004
[164] https://www.taiwannews.com.tw/en/news/3791935
[165] https://www.banking.gov.tw/en/home.jsp?id=42&parentpath=0,3&mcustomize=onemessage_view jsp&dataserno=201801190003&aplistdn=ou=crime,ou=one,ou=english,ou=ap_root,o=fsc,c=tw&dtable=Crime
[166] https://www.lexology.com/library/detail.aspx?g=644356dc-6da9-4fc8-ad3e-1deb18f48848
[167] http://www.winklerpartners.com/?p=7808
[168] https://uk.practicallaw.thomsonreuters.com/5-578-3485?transitionType=Default&contextData=(sc. Default)&firstPage=true&comp=pluk&bhcp=1#co_anchor_a376265

Penalties

Regulatory bodies are able to enforce the PDPA on private sector organisations and order them to remedy violations. If this does not occur, an administrative fee of between NT$20,000 and NT$500,000 may be applied. The FSC has powers to fine according to the PDPA, but may also find the organisation to be in violation of its internal regulatory controls. As such, higher fines may be applied to decisions made by the FSC.

Offence	Applicability	Penalties	Imprisonment
Administrative sanctions	Data users	NT$20,000-NT$200,000	N/A
Criminal sanctions	Data users	Up to NT$1,000,000	5 years

Relevant laws, directives and terminology reference

Law/Decree	Industry	Responsible ministry	Applicability
Personal Information Protect Act	All	Ministry of Justice	All
Employment Service Act	All	Ministry of Justice	All
Freedom of Government Information Law	Government	Ministry of Justice	Government agencies disclosing personal information
Financial Holding Company Act	Banking and Finance	Financial Supervisory Commission	Banks, insurance companies and securities firms under the Act[169]
Medical Care Act	Medical	Ministry of Health and Welfare	Any institution in which physicians practice medicine[170]
Act Governing Electronic Payment Institutions	Banking and Finance	Financial Supervisory Commission	Electronic payment institutions as defined under the Act[171]
Human Biobank Management Act	Medical and Sciences	Ministry of Health and Welfare	Biobank operators[172]
Pharmaceutical Affairs Act	Medical and Sciences	Ministry of Health and Welfare	Pharmaceutical organisations[173]

[169] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380112
[170] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=L0020021
[171] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380237
[172] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=L0020164
[173] https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=L0030001

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
Non-government agency	all persons, juridical persons or groups other than those that are government agencies
Government agency	agency or administrative juridical person at the central or local government level which may exercise sovereign power
Organisation	in this report, refers to any non-government agency or government agency
COVID-19	Coronavirus Disease 2019

Thailand

The Personal Data Protection Act (PDPA), effective since 27 May 2019, is the primary privacy law in Thailand. Organisations had one year to become compliant with the legislation. Thailand also has sector-specific privacy laws and regulations, including those covering anti-money laundering, which provide protection for specific types of information.

The Cabinet of Thailand is considering a royal decree that seeks to postpone most provisions of the PDPA to May 2021.[174] The legislation would defer most of the sections in PDPA act, but not sections 1 and 4 which cover the appointment of members in the Personal Data Protection Committee (PDPC) and the establishment of the Office of the Committee.

Primary legislation: Personal Data Protection Act B.E. 2562 (2019) (PDPA)

Key considerations:

Trends to consider for the Thai market include:

Extraterritorial reach: Data controllers and data processors will be subject to the PDPA where their processing activities relate to offering goods or services or monitoring the behaviour of data subjects in Thailand, even where the controller or processor is not located in Thailand.

Digitisation: The current vision for Thailand's economic growth, Thailand 4.0,[175] seeks a move towards a digital economy. Part of this initiative involves amending the Electronic Transaction Act for e-signatures and publishing a Digital ID Bill for digital authentication.

[174] https://www.bangkokpost.com/business/1917660/pdpa-delay-decree-going-before-cabinet
[175] https://www.boi.go.th/upload/content/Thailand,%20Taking%20off%20to%20new%20heights%20@%20belgium_5ab4e8042850e.pdf (Thai).

Definition of personal data

- Personal data means any information relating only to a (currently) living person which enables the identification of such person, directly or indirectly
- Sensitive data means personal data pertaining to race, ethnic origin, political opinion, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health, disability, trade union affiliation, genetics or biometrics. Sensitive data cannot be collected without the explicit consent of the data subject.[176]

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 PDPA states that information that must be provided to data subjects by data controllers includes:

- details of the personal data to be collected, used or disclosed
- purposes of collection for use or disclosure of the personal data, including the legal basis for the collection (e.g. no consent required)
- data subjects' rights e.g. the right to erase, object, withdraw, etc.
- the data retention period
- the categories or entities, either as an individual or organisation, to which the personal data will be disclosed
- contact details of the data controller or its representative and the Data Protection Officer (DPO).

A data controller is obliged to inform data subjects of the possible consequences of not providing their personal data and whether such provision is a statutory or contractual requirement, or a requirement to enter into a contract. Even if the data subject has consented to the transfer of their personal data outside Thailand, a data controller must inform the data subject of any inadequate privacy safeguards they are aware of in the destination country or international organisation to which the data is to be transferred.

Collecting sensitive data without consent is prohibited, unless it is necessary to:

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

Use and disclosure

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

- relating to scientific, historical or statistical research
- for lawful investigation by officials
- to prevent danger to a person's life or health
- already 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 accord with its original purpose at the point of collection and with consent from the data subjects.

[176] Section 26, PDPA- https://www.etda.or.th/app/webroot/content_files/13/files/The%20Personal%20Data%20Protection%20Act.pdf (English)

Data retention and destruction[177]

A data controller is obliged to have a system in place to erase or destroy the personal data when:

- the retention period ends
- the personal data becomes irrelevant and is no longer required for processing
- the personal data collected is more than necessary for processing to meet the requirements of the data controller and the purpose of collecting the personal data
- the data subject has requested it to do so
- the data subject withdraws their consent.

However, destruction is not required under certain conditions, including where the data is kept to prove a legal claim, or is necessary for freedom of information or in the 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 personal data
- **request access** to their personal data
- **data portability** where data subjects can ask for a copy of their data in a format which is readable or commonly used by automatic tools or equipment, and can be used or disclosed by automated means
- **request** their personal data be erased when the controller does not comply with the PDPA. Data subjects can request that their personal data be deleted, destroyed, temporarily suspended or anonymised
- **restrict further processing** of their personal data by objecting to its collection, use and disclosure
- **seek correction** of their personal data.

Security

An organisation must implement appropriate security measures to prevent the loss, unauthorised access, use, alteration or disclosure of personal data. The security measures must be reviewed when necessary or when technology changes to ensure an appropriate level of security is maintained. Moreover, the data controller shall maintain security records (in written or electronic form) in order to enable the data subject and the Office of the Personal Data Protection Committee (PDPC) to inspect the records.

Data breach notification

Under the PDPA, there is a mandatory requirement to report data breaches to the PDPC and to notify the affected data subjects.

PDPA	
Threshold for reporting	• to the PDPC if the number of affected data subjects is above a prescribed number to be announced by the PDPC • to data subjects if the personal data breach is likely to result in a high risk to the rights and freedoms of the persons affected.
Time frame	without delay and, where feasible, within 72 hours of becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedom of the persons affected.
Who to notify	• affected data subjects • the PDPC in certain circumstances.
Content	awaiting guidance from the PDPC.

[177] Section 37(3), PDPA

Cross-border data transfer[178]

Should the data controller send or transfer personal data across borders, the destination or international organisation require adequate data protection standards. These standards are not to be used as a qualifier for transferring data abroad where the following apply:

- the transfer is made to comply with the law
- the transfer is necessary for a contract to which the data subject is a party
- the transfer is at the request of the data subject prior to entering into a contract
- the transfer is to comply with a contract between the data controller and other persons or juristic persons in the data subject's interests
- the transfer is to prevent or suppress danger to the life, body, or health of the data subject or other persons when the data subject is incapable of giving the consent at such time
- the transfer is necessary in relation to substantial public interest
- a data controller or data processor in the Kingdom of Thailand has a personal data protection policy regarding the sending or transferring of personal data to another data controller or data processor outside Thailand in the same affiliated business, or group of undertakings, in order to jointly operate that business or group of undertakings
- the data subject's consent has been obtained
  - however, if the data controller is aware of any inadequate privacy safeguards in the destination country or organisation, they must inform the data subject even if the subject has consented to the transfer of their personal data outside Thailand.

Where the personal data protection policy has been reviewed and certified by the Office of the Data Protection Committee, the personal data may be sent or transferred to a foreign country as long as it accords with the Committee's review and certification policy.

Governance

The data controller and the data processor are obliged to designate a data protection officer if:

- they are a public authority as prescribed and announced by the Committee
- their collection, use, or disclosure of personal data should be regularly monitored due to processing large volumes of personal data being
- their core activity is to collect, use, or disclose personal data.

Regulators and regulatory landscape

The PDPC's roles and responsibilities include 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 is a supporting body acting as an expert committee. Its roles and responsibilities include 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 - A survey conducted by cybersecurity company, ESET, found 58% of respondent organisations in Asia Pacific had suffered a data breach over the past year. Seven countries in Asia Pacific were part of the ESET Asia Pacific Consumer Behaviour Survey, with Thailand reporting the highest rate of data breaches. Virus attacks were the most common complaint for 44% of study participants.[179]

[178] Section 28 and 29 of PDPA
[179] https://www.eset.com/sg/about/newsroom/press-releases1/press-releases/eset-apac-consumer-behaviour-survey-reveals-58-of-apac-respondents-have-experienced-a-data-breach-i/

Penalties

Non-compliance with the PDPA can amount to:

- administrative fines up to ฿5 million
- criminal penalties for directors held personally liable for non-compliance with imprisonment up to one year and/or fines up to ฿1 million
- punitive damages up to twice the amount of actual damages.

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

Relevant laws, directives and terminology reference

Law/directive	Industry	Regulator	Applicability
Constitution 2017[180]	All	N/A	All
Thai Civil and Commercial Code[181]	All	N/A	All
Official Information Act 1997[182]	Public	N/A	State agencies
The Statistics Act 2007[183]	Public	N/A	National Statistics Office and other responsible agencies
Notification on the Electronic Transactions Commission on Policy and practice Statement on Personal Data Protection of a Government Agency B.E. 2553 2010[184]	Public	N/A	Government agencies
Telecommunications Business Act 2001[185]	Telecommunications	Office of The National Broadcasting and Telecommunications Commission	Licensed telecommunication businesses

[180] http://web.krisdika.go.th/data/law/law1/%c306/%c306-10-2560-a0003.pdf (Thai), http://web.krisdika.go.th/data/outsitedata/outsite21/file/Constitution_of_the_Kingdom_of_Thailand.pdf (official English translation).
[181] http://web.krisdika.go.th/data/law/law4/%bb03/%bb03-20-9999-update.pdf (Thai), http://thailaws.com/law/t_laws/TCCC-book5.pdf (unofficial English translation).
[182] http://web.krisdika.go.th/data/law/law2/%a203/%a203-20-2540-001.pdf (Thai), http://www.krisdika.go.th/wps/wcm/connect/b837b0804ba4d080a47ba78b0853d392/OFFICIAL_INFORMATION_ACT%2C_B.E._2540.pdf?MOD=AJPERES&CACHEID=b837b0804ba4d080a47ba78b0853d392 (official English translation).
[183] http://web.krisdika.go.th/data/law/law2/%ca17/%ca17-20-2550-a0001.pdf (Thai), http://thailaws.com/law/t_laws/tlaw0416.pdf (unofficial English translation).
[184] http://web.krisdika.go.th/data/law/law2/%c763/%c763-2e-9998-update.pdf (Thai), https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2559/EngPDF/25590076.pdf (unofficial English translation).
[185] http://web.krisdika.go.th/data/law/law2/%a1110/%a1110-20-9999-update.pdf (Thai) http://www.krisdika.go.th/wps/wcm/connect/46c2c6004b9e8d2a8809fdea72b7e938/TELECOMMUNICATIONS+BUSINESS+ACT%2C+B.E.+2544+%282001%29.pdf?MOD=AJPERES&CACHEID=46c2c6004b9e8d2a8809fdea72b7e938 (unofficial English translation).

Law/directive	Industry	Regulator	Applicability
Broadcasting and Television Business Operation Act 2008[186]	Telecommunications	Office of The National Broadcasting and Telecommunications Commission	Sound and television broadcasting businesses
Financial Institutions Business Act 2008[187]	Financial	Bank of Thailand	Financial businesses
Credit Information Business Act 2002[188]	Financial	National Credit Bureau Company Limited	Credit information companies, data controllers and processors

Terminology	Definition
Data controller	natural or legal person who solely, or jointly, is responsible for information processing
Data processor	natural or legal person who processes information on behalf of an information controller
Personal data	any information relating to a person, which enables their identification either directly or indirectly, but not including information of a deceased person.

[186] http://web.krisdika.go.th/data/law/law2/%a1129/%a1129-20-2551-a0001.pdf (Thai), http://www.krisdika.go.th/wps/wcm/connect/d51cc5004ba4484f9efcbf8b0853d392/BROADCASTING+AND+TELEVISION+BUSINESSES+ACT%2C+B.E.+2551+%282008%29.pdf?MOD=AJPERES&CACHEID=d51cc5004ba4484f9efcbf8b0853d392 (unofficial English translation).
[187] http://web.krisdika.go.th/data/law/law2/%b812/%b812-20-9999-update.pdf (Thai), ht https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/SiteAssets/Law_E24_Institution_Sep2011.pdf (unofficial English translation).
[188] http://web.krisdika.go.th/data/law/law2/%a1112/%a1112-20-9999-update.pdf (Thai), http://www.krisdika.go.th/wps/wcm/connect/4127f68043c803f4bcadfc25b7244636/CREDIT+INFORMATION+BUSINESS+OPERATION+ACT%2C+B.E.+2545+%282002%29.pdf?MOD=AJPERES&CACHEID=4127f68043c803f4bcadfc25b7244636 (unofficial English translation).

Vietnam

Vietnam does not have a comprehensive legislative regime responsible for privacy.

In February 2020, the Ministry of Public Security (MPS) announced it had completed a draft dossier on a decree on personal data protection, known as the Draft Decree. MPS is currently seeking comments and expects to submit the Draft Decree to the Government in 2020.[189]

The Law on Network Information Security (86/2015/QH13), widely referenced as the Law on Cyber Information Security (86/2015/QH13) (LCIS), provides the requirements to protect personal information. These apply to individuals and organisations engaged in information technology application and development activities in Vietnam.

Primary legislation: Law on Network Information Security (86/2015/QH13) [LCIS]

Key considerations:

Increased priority for cybersecurity: In 2018, Vietnam enacted the Law on Cybersecurity (24/2018/QH14), which increases the power granted to the state to investigate users and to censor content published online by individuals.

Enforcement: The Ministry of Information and Communications can examine, inspect and review complaints and other suspected violations of the LCIS.

Data localisation: The new Law on Cybersecurity establishes stricter requirements for foreign service providers operating in Vietnam, including data localisation in certain circumstances. The Draft Decree also seeks to address 'registration of the transfer of personal data of Vietnamese citizens overseas.'

Draft decree: The Draft Decree defines personal data as an individual's information data in the form of symbols, alphabetic letters, numbers, images, sounds or other similar forms. It proposes various provisions to cover:

- protection, lawful processing, collection purpose and limits, consent requirements, cross-border data transfers, quality and validity preservation and security measures
- access and a data subject's right to access
- the data subject's rights to transparency around their personal data processing
- the obligation for data processors to immediately delete personal data that is unnecessary, unless it is otherwise regulated by law
- offshore personal data processors that may be required to appoint a data privacy representative in Vietnam.

[189] https://rouse.com/insights/news/2020/new-draft-decree-on-personal-data-protection-in-vietnam

Definition of personal information[190]

Personal information is defined broadly by the LCIS Law as 'information associated with the identity of a specific person'. This includes any information that relates to a data subject's:

- personal life including name, date of birth, address, telephone number, identification number, or email address
- personal or family secrets
- personal communications, including written correspondence and telephone call content.

Collection, use and disclosure of personal information

When collecting or using personal information, the LCIS requires organisations and individuals to:

- collect personal information only after obtaining the consent of the information owner on the collection's scope, purpose and use
- obtain the personal information owner's agreement to use their information for any purpose other than that it was originally collected
- not share or disperse the collected, accessed or controlled personal information with any third party, unless agreed to by the personal information owner or requested to by competent state bodies.

Direct marketing
The LCIS prohibits organisations and individuals from sending commercial information to a recipient's electronic address without their prior consent, request, or if the recipient refuses it, except where the recipient is obliged to receive the information under current law. The Law on Protection of Consumers' Rights also prohibits the harassment of consumers through marketing goods and services contrary to their wishes.[191]

Data retention and destruction

The Law on Cybersecurity requires local and foreign enterprises that provide telecommunication and other related information technology and communication services in Vietnam, to store personal data in Vietnam for a period specified by the Government.

Individual rights
The LCIS provides that the personal information owner has the right to require any organisation or individual handling its personal information, to provide their information on request.

[190] https://www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf
[191] https://aseanconsumer.org/file/pdf_file/Vietnam%20Legislation%20-%20Law%20on%20Protection%20of%20Consumer%20(english).pdf

Data security

Before processing personal data of a data subject, the LCIS requires the processor to provide adequate protection for the personal data as per the technical standards and norms of network information security system detailed in Chapter V of the LCIS (technical standards). The LCIS requires organisations to take appropriate managerial and technical measures to protect any collected and stored personal information, and take the necessary remedial actions to mitigate any risks to it.

According to the LCIS a data processor must:[192]

- publish its security policy, outlining the design, construction, operation, management, use, upgrade, and deconstruction of the information system
- apply appropriate technical and management measures according to the security standards for information systems that both maintain the information system and minimise any risk of a security incident
- examine and supervise compliance with the organisation's security policy and evaluate the effectiveness of applied technical and management measures
- supervise the protection of the information system.

The LCIS requires information systems to be classified according to a rating between 1 and 5, to manage any likely impact in the event of sabotage to the system, as follows in the table below.

Level	Description of classification
1	a sabotaged information system will damage the legitimate rights and benefits of organisations and individuals, but not public benefits, social order, safety, national defence or security
2	a sabotaged information system will severely damage the legitimate rights and benefits of organisations, individuals and public benefits, but not social order, safety, national defence or security
3	a sabotaged information system will severely damage production, public benefits and social order or damage safety, national defence or security
4	a sabotaged information system will extremely damage public benefits, social order or safety, or severely damage national defence or security
5	a sabotaged information system will extremely damage national defence or security.

[192] https://www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf

Data localisation

The new Law on Cybersecurity (24/2018/QH14) includes a requirement for domestic and foreign service providers that process personal information of service users in Vietnam to store data locally.[193] The supporting draft Decree clarifies that local and foreign service providers, potentially subject to data localisation, can include those providing services such as social media, email, online payments, online games and telecommunications.[194]

Censorship

The new Law on Cybersecurity (24/2018/QH14) also requires local and foreign service providers to verify the information in users' accounts, provide user information to authorities for investigation in certain circumstances, and censor and block information, and users, responsible for certain types of information. For example this can include information deemed to be inciting opposition to the Government or which 'undermines national solidarity'.[195]

Regulators and regulatory landscape

There is no established privacy or data protection regulator in Vietnam. The Ministry of Information and Communications is primarily responsible for the implementation of the LCIS but may work in conjunction with other ministries relating to other information technology and e-commerce laws. Its responsibilities cover regulating the press, publishing, posts, telecommunications, radio frequency, information technology, electronics, broadcasting, media, foreign information, domestic information, national information and communication infrastructure and managing related public services on behalf of the Government.

Data breach notification

Notification to the Commissioner: Data breach notification to a regulator or data subjects is not mandatory. The limited guidance that has been provided is outlined below.

Voluntary guidance

Threshold for reporting	data breach reporting is required when '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, responsible for the Decree on e-Commerce
Content	there is no specific requirement relating to the content to be included in notifications.

Data transfer

There are no specific restrictions on the transfer of personal information in Vietnam. However, article 17 of the LCIS relating to the collection and use of personal information, requires that organisations should not share or disperse the collected, accessed or controlled personal information to any third party, unless agreed by the personal information owner or requested by competent state bodies.[196]

[193] https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/249980/q/WT/TPR/OV21.pdf
[194] https://www.reuters.com/article/us-vietnam-socialmedia-exclusive/exclusive-vietnam-cyber-law-set-for-tough-enforcement-despite-google-facebook-pleas-idUSKCN1MK1HL
[195] http://moj.gov.vn/en/Pages/Activities-of-public-administrative-and-justice-reform.aspx?ItemID=3255
[196] http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf

Cases

- **2019 -** Japan's Toyota Motor Corporation detected unauthorised access on servers at its subsidiaries in Vietnam. Toyota released a notice that the company acknowledged the possibility that there were entities in Vietnam that were targeted by a cyberattack and that some of its customer data may have been potentially accessed.[197]
- **July 2016 -** Personal data was stolen and leaked over the internet after the Vietnamese airline's website was subject to a cyberattack by a group of hackers.[198]

Penalties

The LCIS provides that violations of the law will be disciplined, based on their nature and severity, and will include potential administrative sanctions, examination for penal liability and, if responsible for causing damage, liability to pay compensation.

Other considerations

Exemptions: The LCIS provides the following exemptions from the data protection rules:

- personal data processed by a competent authority or based on a decision made by them
- personal data being processed to ensure national security, protect national defence, maintain public order or meet non-commercial objectives in accordance with relevant laws.[199]

The draft decree proposes that an exception may be given when obtaining consent for collecting personal data, such as when disclosures are made to the media in the public's interest.

Relevant laws, directives and terminology reference

Law/Decree	Industry	Responsible ministry	Applicability
Law on Network Information Security (86/2015/QH13)	Comprehensive	Ministry of Information and Communications[200]	Any Vietnamese agency, organisation, or individual, or foreign organisation and individual in Vietnam directly involved in or related to network information security activities in Vietnam[201]
Law on Protection of Consumers' Rights (59/2010/QH12)	Consumer	Ministry of Trade and Industry[202]	Consumers, organisations or individuals trading goods, services, or agencies, organisations or individuals involved in activities to protect the interests of consumers in Vietnam

[197] http://www.toyotavn.com.vn/en/news/press-release/854/notice-on-a-cyberattack-targeting-toyota
[198] https://en.wikipedia.org/wiki/Vietnamese_airports_hackings#:~:text=On%2029%20July%202016%2C%20a,Airport%2C%20posting%20derogatory%20messages%20against
[199] https://www.amchamvietnam.com/wp-content/uploads/2019/05/Data-Protection-in-Vietnam-Overview-April-2019.pdf
[200] http://english.mic.gov.vn/Pages/home.aspx
[201] http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf
[202] http://www.moit.gov.vn/

Law/Decree	Industry	Responsible ministry	Applicability
Law on Information Technology (67/2006/QH11)	Comprehensive	Ministry of Information and Communications[203]	Vietnamese and foreign organisations and individuals engaged in information technology application and development activities in Vietnam
Decree on E-Commerce (52/2013/ND-CP)	E-commerce	Ministry of Industry and Trade[204]	Organisations and individuals conducting part or all the electronic commercial activity connected with the internet, mobile telecommunications network or other open networks
Law on Cybersecurity (24/2018/QH14)	Online Service Providers	Cybersecurity Task Force, under the Ministry of Public Security [205]	Vietnamese and foreign enterprises providing telecom networks, internet and other value-adding services in cyberspace in Vietnam
The Press Law No. 103/2016/QH13	Media / Press	Ministry of Information and Communications	Governs the press, including citizens' rights to freedom of press and freedom of speech in the press and the rights and obligations of agencies, organisations, and individuals involved in the media industry
The Civil Code of Vietnam (33/2005/QH11)	Comprehensive	N/A	Specifies that: • an individual's rights to personal secrets shall be respected and protected by law • collecting and publishing information and materials on the private life of an individual must be only with their consent • in cases where a person has died, lost their civil capacity to act, or is under a full 15 years of age, the consent of his or her father, mother, wife, husband, adult children or representative is required, except where the decision to collect and publish information and materials is made by a competent agency or organisation • an individual's letters, telephones, telegrams and other electronic information should be guaranteed safety and confidentiality.

[203] http://www.moj.gov.vn/vbpq/en/lists/vn%20bn%20php%20lut/view_detail.aspx?itemid=4761
[204] http://vietnamlawenglish.blogspot.com/2013/05/vietnam-decree-no-522013nd-cp-on-e.html
[205] http://moj.gov.vn/en/Pages/Activities-of-public-administrative-and-justice-reform.aspx?ItemID=3255

Law/Decree	Industry	Responsible ministry	Applicability
The Law on Telecommunications No. 41/2009/QH12	Organisations, individuals, organisations and foreign individuals involved in or related to telecommunication activities in Vietnam	The Ministry of Information and Communications	this law regulates telecommunications activities and the rights and obligations of those working in the telecommunication industry
The Law on Credit Institution No. 47/2010/QH12	Credit institutions, foreign bank branches and representative offices of foreign credit institutions and other foreign institutions engaged in banking	Ministry of Finance	this law governs credit institutions establishing and operating in Vietnam.

Terminology	Definition
Personal data processor	is a legal entity, natural person, or branch of a foreign company or state authority or local authority that processes personal data
COVID-19	Coronavirus Disease 2019 as defined by the World Health Organisation
Information system	refers to any assembly of hardware, software or database that facilitates the supply, communication, collection, handling, storage and/or exchange of network information.

Comparison matrix

This table is a visual comparison of selected privacy elements covered in the Asia Pacific region at the time of writing. It is designed as a guide and not an exhaustive list of locations or attributes.

S.No.	Location	Definition of personal information/data		Collection & 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		
1	Australia	✓	✓	✓	✓	✓	✓	×	×	×	✓	✓	×	✓	×
2	Bangladesh	✓	×	✓	✓	✓	×	×	×	×	×	×	×	✓	×
3	Brunei Darussalam	✓	×	✓	✓	✓	✓	×	×	×	✓	×	×	✓	×
4	Cambodia	×	×	×	×	×	×	×	×	×	×	×	×	×	×
5	China	✓	×	✓	✓	✓	✓	×	×	×	✓	✓	×	✓	×
6	Hong Kong	✓	×	✓	✓	✓	✓	×	×	×	✓	•	✓	✓	×
7	India	✓	✓	✓	✓	✓	✓	•	•	•	✓	•	✓	✓	•
8	Indonesia	✓	•	✓	✓	✓	✓	✓	•	✓	✓	✓	×	✓	•
9	Japan	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓	×
10	Lao PDR	✓	×	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	×
11	Malaysia	✓	✓	✓	✓	✓	✓	×	×	×	✓	×	×	✓	×
12	Mongolia	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×
13	Myanmar	×	×	×	✓	×	×	×	×	×	×	×	×	×	×
14	New Zealand	✓	×	✓	✓	✓	✓	×	×	×	✓	•	✓	✓	✓
15	Papua New Guinea	×	✓	×	×	×	×	×	×	×	×	×	×	×	×
16	The Philippines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
17	Singapore	✓	×	✓	✓	✓	✓	✓	✓	•	✓	•	✓	✓	✓
18	South Korea	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	×	✓	✓
19	Sri Lanka	•	•	•	•	•	•	•	•	×	•	•	×	•	•
20	Taiwan	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	×	✓	×
21	Thailand	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
22	Vietnam	✓	×	✓	✓	•	✓	×	×	×	✓	×	✓	×	×

Regulatory landscape table

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

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 A$2.1 million and enforceable undertakings
Bangladesh	Cybersecurity	Yes	Digital Security Agency	Imprisonment up to 5 years and fines ranging from ৳500,000 to ৳1,000,000
Brunei Darussalam	Sectoral	No	Minister at the Prime Minister's Office	None. Criminal and government investigations and prosecution may be initiated
Cambodia	Sectoral	Yes	None	None
China	Cyber and Information security law	Yes	Cyberspace Administration of China	Fines of up to ¥1 million
Hong Kong	Comprehensive	Yes	The Office of the Privacy Commissioner for Personal Data	Financial penalties of up to HK$1 million and imprisonment for up to 5 years
India	Information Technology law	Yes	Ministry of Electronics and Information Technology	Imprisonment of up to 3 years and fines up to ₹500,000 Personal liability and/or criminal sanctions
Indonesia	Data Protection and Information Technology law	Yes	Ministry of Communication and Information Technology	Administrative sanctions and criminal liabilities
Japan	Comprehensive/EU adequacy	Yes	Personal Information Protection Commission	Up to 1 year imprisonment or a maximum fine of ¥1 million
Lao People's Democratic Republic	Information security law	No	Ministry of Posts and Telecommunications	Personal liability, criminal sanctions and/or fine of ₭15 million

Location	Regulation	Constitutional right to privacy	Regulator	Maximum penalty for privacy law breach
Malaysia	Comprehensive	No	Personal Data Protection Department and Malaysian Communications and Multimedia Commission	Fine not exceeding RM300,000 and/or imprisonment for a term not exceeding 2 years
Mongolia	Sectoral	Yes	Non-privacy specific	Criminal and administrative sanctions
Myanmar	Sectoral	Yes	Ministry of Communications and Information Technology	Imprisonment up to 3 years and a fine up to K1.5 million
New Zealand	Comprehensive/ EU adequacy	No	Privacy Commissioner's Office	Damages up to NZ$350,000
The Philippines	Comprehensive	Yes	National Privacy Commission	Imprisonment up to 6 years and/or fine up to ₱4 million
Papua New Guinea	Information security law	Yes	None	None
Singapore	Comprehensive	No	Personal Data Protection Commission	Imprisonment up to 1 year and/or fine up to S$1 million
South Korea	Comprehensive	Yes	Personal Information Protection Commission	Fines of up to ₩100 million and imprisonment of up to 10 years
Sri Lanka	Information security law	No	Information and Communication Technology Agency	None
Taiwan	Comprehensive	Yes	Personal Data Protection Office	Fines ranging from NT$20,000 to NT$500,000
Thailand	Comprehensive	No	Personal Data Protection Committee	Fines up to ฿5 million and/or imprisonment up to 1 year
Vietnam	Information security law	Yes	Ministry of Information and Communications	Administrative sanctions, penal liability and monetary compensation.

Table of primary privacy regulations and regulators

Location	Current legislation	Regulator
Australia	Privacy Act 1988 (Cth)	Office of the Australian Information Commissioner https://www.oaic.gov.au/
Bangladesh	Digital Security Act 2018	Digital Security Agency http://www.btrc.gov.bd/useful-links/post-telecommunication-division-ministry-post-telecommunications-and-information
Brunei Darussalam	Data Protection Policy 2014	Minister at the Prime Minister's Office http://www.pmo.gov.bn
Cambodia	The Constitution of the Kingdom of Cambodia and the Civil Code of Cambodia, 2007 (the Civil Code)	None
China	People's Republic of China Cybersecurity Law 2017	Cyberspace Administration of China http://www.cac.gov.cn/
Hong Kong	Personal Data (Privacy) (Amendment) Ordinance 2012	The Office of the Privacy Commissioner for Personal Data https://www.pcpd.org.hk/
India	Information Technology Act, 2000	Ministry of Electronics and Information Technology https://meity.gov.in/
Indonesia	• Government Regulation No. 71 of 2019 (GR 71/2019) • Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its amendment Law No. 19 of 2016 • MOCI Regulation No. 20 of 2016 (Protection of Personal data in an Electronic System) (MOCI Law)	Ministry of Communication and Information Technology https://www.kominfo.go.id/
Japan	Act on the Protection of Personal Information, 2017 (APPI) & Amended APPI 2020	Personal Information Protection Commission https://www.ppc.go.jp/en/
Lao People's Democratic Republic	Law on Electronic Data Protection, 2017	Ministry of Posts and Telecommunications https://www.mpt.gov.la/

Location	Current legislation	Regulator
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	None
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 & Privacy Act 2020	Privacy Commissioner's Office https://www.privacy.org.nz/
Papua New Guinea	Privacy Communications Act, 1973, Constitution of the Independent State of Papua New Guinea and National Information and Communications Tech Act, 2000	None
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 Data Protection Act, 2010	Personal Data Protection Office
Thailand	The Personal Data Protection Act B.E. 2562 (2019) (PDPA)	Personal Data Protection Committee
Vietnam	Law on Network Information Security (86/2015/QH13) [NIS Law] also known as Law on Cyber Information Security (86/2015/QH13) (LCIS)	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:

Beatrix Ariane
Jakarta

Ambika Bahadur
New Delhi

Marie Chami
Sydney

Sung Kyo Cho
Seoul

Nakul Chopra
New Delhi

Paras Chugh
New Delhi

Abhishek Dubey
Auckland

Karen Grieve
Sydney

Ho Kyoo Hahn
Seoul

Arvin Raj Kumar Kantha
Kuala Lumpur

Eric Leo
Sydney

Brad Lin
Hong Kong

Han Lin
Taipei

Kumar Manthri
Colombo

Toshiyuki Oba
Tokyo

Rajesh Pradhan
Auckland

Kartikeya Raman
New Delhi

Ajay Rana
Yangon

Herbert Rollom
Taguig

Hatty Hoi Ting Siu
Hong Kong

Monai Supanit
Bangkok

Maurya Velpula
Kuala Lumpur

Rishi Wadhwa
New Delhi

Manna Wu
Hong Kong

Patty Fei Jia Yang
Beijing

Key contacts

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

Manish Sehgal
Asia Pacific Cyber Data & Privacy leader
+91 124 679 2723
masehgal@deloitte.com

James Nunn-Price
Asia Pacific Cyber leader
+61 2 9322 7971
jamesnunnprice@deloitte.com.au

Australia
Daniella Kafouris
Partner
+61 3 9671 7658
dakafouris@deloitte.com.au

New Zealand
Faris Azimullah
Partner
+64 9 303 0842
fazimullah@deloitte.co.nz

Chinese Mainland/Hong Kong
Frank Xiao
Partner
+86 108 512 5858
franxiao@deloitte.com.cn

Eva Yee Ngar Kwok
Partner
+852 2852 6304
evakwok@deloitte.com.hk

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

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

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

Taiwan
Max Y. Lin
Partner
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

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

Deloitte.