netskope pwc

White Paper

Privacy and Data Protection for Cross-Border Data Transfers in the Asia Pacific Region

Security

Reform

Cloud security and cross-border transfers

With many businesses moving their data into the cloud and worldwide public cloud revenue predicted to top more than USD500 billion this year, cloud security and associated regulations remain top of mind for CEOs globally.

Results from PwC's 26th Annual Global CEO survey revealed that APAC CEOs consider "cyber risks" to be the fourth most pressing concern or material risk to business growth. In addition, the survey also revealed that cyber risks will be a particular area of focus for larger companies over the next five years.

Cloud security and personal data protection also continue to be key priorities for governments and regulators around the world. The concepts of "data sovereignty" and "data localisation" are becoming more prevalent and sovereign nations are more attuned to the expectation and desire of their citizens for the government to play a greater role in the protection of their personal data.

This has resulted in an increasing number of reforms and new laws or regulations being introduced in certain jurisdictions across the APAC region that relate specifically to storing data in the cloud and / or transferring personal data across international borders. At the same time, more guidelines have been issued to assist organisations engaging in cross-border transfers.

With multiple jurisdictions increasing the maximum penalty for breaches of privacy and data protection laws, now more than ever, senior leadership of multinational organisations need to have a comprehensive understanding of how data protection laws apply to their business operations across the globe and stay up to date with the constantly evolving regulatory landscape.

The regulatory landscape for cross-border data transfers in the APAC region

The governance of cross-border data flows in the APAC region is quite fragmented and the body of national laws and regulations on data protection are widespread and wide ranging.

This patchwork of laws often results in conflicting approaches to the implementation and enforcement of cross-border data transfers within the APAC region, posing challenges for businesses and regulatory authorities. That is, what may be a simple process to transfer data outside of one jurisdiction could also be a very complex process in another requiring careful consideration and planning. To help highlight this, this publication provides an overview of some key aspects of the laws or regulations governing cross-border data transfers across 14 APAC countries.

In the past year, several countries have introduced their first comprehensive data privacy laws. For example, India, Vietnam, and Indonesia have respectively issued their long-awaited first-ever comprehensive regulations on data privacy. This shows that governments in the APAC regions see a dire need for regulatory uplift and alignment with their global counterparts. Jurisdictions with more mature privacy regimes continue to amend and tighten their existing privacy laws and regulations.

Key challenges for APAC organisations

When it comes to transferring data across borders, some of the challenges organisations are facing in the APAC region include:

- the impact of the broad extra-territorial application of the EU GDPR across the globe;
- countries restricting the transfer of data to organisations located in "approved" (i.e. "whitelist") recipient countries that are deemed to have adequate data protection laws in place;
- requirements to inform data subjects of the particulars of a transfer and obtain their consent prior to the transfer;
- obligation to notify and / or obtain approval from regulators or relevant supervisory authorities before undertaking a transfer; and
- requirements to implement data security measures in order to protect data before, during, and after the transfer takes place.

Are the laws of some countries more stringent than others?

There are some countries within the APAC region that impose greater restrictions on the transfer of personal data to other nations, especially for data that may impact national security and / or sensitive personal data.

For example, in China, security assessments must be conducted and approval obtained from industry regulators, before data can be transferred outside of mainland China. For some industries, such as those operating in the finance sector, this makes the transfer of data outside of China almost impossible. In the past year, Chinese regulators have issued detailed measures on security assessment, security certification and the standard contract for cross-border transfer of personal information, providing more guidance for organisations to comply with cross-border data transfer requirements. However, only recently, Chinese regulators have proposed for consultation, draft regulations aimed at easing some requirements and streamlining the vigorous security requirements pertaining to cross-border transfer of personal information under certain circumstances.

Vietnam's new law also includes restrictions on the transfer of Vietnamese citizens' personal data out of Vietnam. An organisation transferring data abroad must prepare a cross-border transfer impact assessment and submit it to the competent authority within 60 days.

In Malaysia, a data user / processor must not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister (or an exception applies). Also in Malaysia, personal data transferred to third-party service providers located outside of Malaysia will require due diligence to be performed and contractual obligations imposed on third parties to protect personal data.

Meanwhile, Australia is expected to see significant reforms to its privacy laws following the Australian Government's response to the proposals in the Privacy Act Review Report.

To further promote interoperability, some countries voluntarily signed up to the APEC Cross-Border Privacy Rules (**CBPR**) system, which is a data privacy certification system that governments can join to enable privacy-respecting data flows among other APEC economies. Each member country determines how it will implement the CBPR system in its own jurisdiction. In some countries, it is seen as best practice, while in others (e.g. Japan), the system has become a basis for cross-border data transfers in compliance with domestic law. The CBPR system does not replace national law nor does it afford

immediate adequacy standards or white-listing. The CBPR merely establishes minimum standards for privacy protections across various jurisdictions by applying set principles and rules. Further, APEC member companies that have had their privacy policies and practices certified under the CBPR system can showcase the certification to other APEC member's companies as an indicator of compliance. There were initially nine participating APEC CBPR system economies (including six APAC region jurisdictions covered in this publication) being, USA, Mexico, Japan, Canada, Singapore, South Korea, Australia, Taiwan, and the Philippines.

The Global Cross-Border Privacy Rules Forum (**Global CBPR Forum**) which expands on the APEC CBPR system was later established to (i) facilitate data protection and free flow of data globally, (ii) share best practices and promote cooperation on data protection, and (iii) achieve interoperability with other data protection frameworks. It is currently made up of the same countries participating in the APEC CBPR systems and additional economies (Bermuda, Dubai, United Arab Emirates, and the UK). A number of global organisations are certified under the APEC CBPR system with others announcing an intention to certify under the Global CBPR system.

Data localisation and sovereignty

There are some countries in the APAC region that have adopted data localisation laws, which typically imposes additional restrictions on cross-border data transfers making it mandatory for organisations to store and / or process data within that country locally.

These laws are often driven by national security or public interest, and relate to specific data (i.e. sensitive data, financial information, etc.). For example:

- "important data" handled by critical information infrastructure operators and large amounts of personal data in China are subject to data localisation requirements; and
- data handled by Electronic Service Providers operating within the public sector in Indonesia are also required to process, manage and / or collect electronic systems and electronic data within the Indonesian jurisdiction.

More commonly, data localisation or data sovereignty requirements are regulated by sector specific data protection provisions. For example, in Vietnam, data localisation requirements are set out in the *Law No. 24/2018/QH14 on Cybersecurity,* while South Korea's *Regulation on Supervision of Electronic Financial Transactions* prescribes that finance companies headquartered in Korea must have their data centre and disaster-recovery centre located in Korea.

There is a global trend towards having stricter data protection obligations in healthcare, IT / cloud services, telecommunications, and banking / financial services industries, presumably due to the more sensitive nature of the data held by organisations in those industries.

Upcoming reform

Many of the APAC regions featured in this publication are either reviewing current data protection legislation to better align with global standards or expectations or seeking to implement new or more consolidated or comprehensive data protection laws. These have resulted from the identification of gaps in local law against the EU GDPR and broader global data privacy law reforms, as well as the changes in the marketplace, consumer expectations and technological advances that have driven the need for better protections of individuals' privacy.

In 2022, a number of countries such as China, have adopted or are in the process of implementing the newly introduced regulations. The past year has also seen enforcement regimes strengthened across various jurisdictions — for example, both Australia and Singapore have increased penalty cap for breach of privacy regulations, whilst other jurisdictions (such as China, Hong Kong, Malaysia, Taiwan) are looking to do the same. Some of the other key themes being seen across these proposed reforms include:

- obligations on organisations to increase transparency and accountability with respect to personal data collection and use;
- requirements to ensure organisations are obtaining express, informed consent from data subjects to the collection and use of personal data;
- imposing restrictions on cross-border data transfers;
- introducing a right to data portability; and
- introducing mandatory data breach notification or reporting obligations.

APAC jurisdictional overviews

This publication contains overviews of the privacy and data protection laws and regulations of 14 APAC regions, namely: Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam.

Each jurisdiction overview contains a high-level summary broken down into the following core focus areas:

- ***Key privacy and data protection laws,*** regulations and guidance that apply in that jurisdiction.
- ***The regulator or authority responsible*** for overseeing compliance with the privacy and data protection laws and regulations.
- ***Data Protection Officer requirements.***
- ***An overview of the scope and extra-territorial application*** of the privacy and data protection laws and regulations, including the definition of personal information, sensitive personal information and other types of information regulated.
- ***Employee data / information*** and whether there are specific consent or notice obligations when collecting or handling such data.
- ***Cross-border data transfer requirements,*** including the existence of data localization / sovereignty laws.
- ***Summary of the legal bases*** for the collection and processing of personal information.
- ***Data security requirements,*** including data minimization obligations.
- ***Data breach notification requirements,*** including the implications for failure to notify.
- ***The rights of individuals in respect of their personal information*** (focusing on the right to deletion, right to access, and right to correction) and whether an individual has the right to take direct action against an organisation for breaches or interferences of their privacy.
- ***Privacy by design and default requirements.***
- ***Enforcement powers of the regulator, fines and penalties*** for breaches or infringements of the privacy and data protection laws (including whether there are specific directors or officers duties relating to privacy).
- ***Snapshot of upcoming reform*** or reviews taking place or anticipated in that jurisdiction.

NETSKOPE | APAC PRIVACY PUBLICATION

AUSTRALIA

KEY PRIVACY / DATA PROTECTION LAWS

The principal privacy legislation is the federal *Privacy Act 1988* (Cth) (**Privacy Act**) which includes the Australian Privacy Principles (**APPs**). The Privacy Act (including the APPs) regulates the handling of "personal information" by private sector organisations (with an annual turnover of AUD 3 million or more). The term "personal information" is broadly defined and includes "information or an opinion" about an individual in any format (including electronic files).

Some Australian States and Territories have their own privacy legislation which oversees the information handling practices of public sector agencies and certain organisations that handle health information (including public and private service providers that interact with the government agencies).

There are also other related data protection laws that may apply in certain circumstances, including the Australian Consumer Law and consumer data rights regime found in the *Competition and Consumer Act 2010* (Cth), the *Spam Act 2003* (Cth), and the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth).

REGULATOR / AUTHORITY

The Office of the Australian Information Commissioner (**OAIC**) is the independent regulatory body with the key responsibility for ensuring the proper handling of personal information under the Privacy Act and protecting individuals' rights to access public information under Australia's Freedom of Information laws. From May 2023, the OAIC consists of three statutory office holders, being the Australian Information Commissioner (as agency head), the Privacy Commissioner and the Freedom of Information Commissioner.

Other regulators or authorities that may oversee "data related matters" include the Australian Competition and Consumer Commission, Australian Tax Office, Australian Communications and Media Authority, Australian Prudential Regulation Authority, Australian Securities and Investments Commission and State / Territory authorities.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

Under the Privacy Act, there is no specific requirement to appoint a DPO or privacy officer for most organisations (with the exception of Commonwealth public sector agencies). Under the *Australian Government Agencies Privacy Code*, relevant public sector agencies are required to appoint a privacy officer, or privacy officers, and ensure that particular privacy officer functions are undertaken.

While the appointment of a DPO or privacy officer is not generally required, the Privacy Act requires an organisation to implement practices, procedures and systems that will ensure its compliance with the Privacy Act and enable it to deal with inquiries or complaints. The appointment of a designated privacy officer may be one of the measures that an entity may implement to comply with this requirement. The OAIC has released guidelines that recommend certain practices, procedures, and systems that

organisations should consider implementing, including (among other things) governance mechanisms such as the appointment of a designated privacy officer.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

As noted above, the Privacy Act regulates the handling of an individual's "personal information" by organisations whether or not that organisation is physically present in Australia or not (i.e. foreign organisations). This means that the Privacy Act also applies to include "foreign" organisations that are deemed to have an "Australian link". For example, the incorporation of an Australian subsidiary by a foreign parent would constitute an Australian link. A foreign organisation that is incorporated outside of Australia will have an Australian link if it carries on a business in Australia whether it has a physical presence in Australia or it collects or holds personal information in Australia.

The extra-territorial application of the Privacy Act has been the subject of a recent Commissioner Determination and Federal Court case involving large, multinational corporations that have no physical presence in Australia. Although the position has not been completely settled and the decisions may be appealed, these determinations provide some guidance in relation to the extra-territorial application of the Privacy Act.

Personal information also includes sensitive information, health information, credit information and tax information.

Sensitive information is defined under the Privacy Act to include information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record, health or genetic information and some aspects of biometric information.

EMPLOYEE DATA / INFORMATION

Currently, there is an "employee records exemption" which exempts private sector employers from having to comply with the Privacy Act obligations when handling employee records in relation to a current or former employment relationship. An "employee record" is a record of personal information relating to the employment of the employee, such as health, performance, disciplinary, payroll, taxation, superannuation, leave, or termination information.

The employee records exemption is narrow in scope and does not apply to an organisation's processing of personal information of job applicants, temporary workers or independent contractors who are not employees, or employees of other entities. The exemption also does not apply to an employee's personal information that is not directly related to the employment relationship.

Where the employee record exemption does not apply, organisations will be required to comply with the APPs when collecting and handling employee personal information. There are currently no specific requirements for obtaining employee consents. However, it is typically more difficult to establish that consent is voluntary and therefore valid in an employment context.

Separately, there are workplace surveillance laws that need to be considered by organisations that conduct surveillance or monitoring of employees.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Before an organisation discloses personal information to an overseas recipient, it must take "reasonable steps" to ensure that the overseas recipient does not breach the Privacy Act requirements.

Organisations that disclose personal information to overseas recipients may be held accountable for any acts or practices of the overseas recipient in relation to the personal information that would breach the Privacy Act.

There are some limited exceptions to the cross-border transfer requirements. For example, where the organisation has a "reasonable belief" that the overseas recipient is subject to a law, or binding scheme, that is substantially similar to the Privacy Act and individuals would have the ability to enforce protection under the law or binding scheme. In addition, restrictions will not apply, if the organisation informs the individual of the overseas transfer and obtains the express consent of the individual to the transfer.

In August 2022, the Australian Government announced that Australia joined the Global CBPR Forum. The CBPR system is a voluntary certification scheme, originally developed in APEC, which enables a business' personal information handling practices to be certified as meeting internationally recognised privacy standards. Australia has been participating in the APEC CBPR system from November 2018. The Global CBPR Forum intends to promote expansion and uptake of the CBPR system globally, disseminate best practices for data protection and interoperability and pursue interoperability with other data protection frameworks. The announcement comes as the Government is working on broader reforms of Australian privacy laws, including several changes to rules on overseas disclosure (more see section "Upcoming Reform").

Additional protective measures for cross-border transfers

Although the OAIC encourages the adoption or implementation of additional measures to protect personal information that is being disclosed to overseas recipients (such as binding corporate rules, standard contractual clauses, etc.), there are no specific obligations on organisations to implement these measures.

As noted above, the organisation must have a reasonable belief that the overseas recipient is subject to a law, or binding scheme, that is accessible by the relevant individual. It is the responsibility of the organisation to be able to justify its reasonable belief. From a practical perspective, this may involve obtaining independent legal advice as evidence of the steps taken to form their view / belief.

Data sovereignty / localisation

Outside of the above cross-border transfer restrictions, there are no specific data sovereignty or localisation requirements (such as governmental consent, approval, or registration requirements) under the Privacy Act.

There are some government policies or industry specific legislation (e.g. telecommunications), that may have an impact on where an organisation chooses or is required to maintain certain information registers or records. The application of these policies / laws would need to be considered on a case-by-case basis, having regard to the industry the organisation operates in and the types of information they collect.

COLLECTION AND PROCESSING OBLIGATIONS

Organisations may only collect personal information that is reasonably necessary for one or more of its functions or activities or if the individual provides their express, informed consent. The collection must only occur by lawful and fair means and directly from the individual, unless an exception applies (i.e. the individual's consent is obtained or the organisation is required or authorised by or under an Australian law, or a court / tribunal order).

SECURITY REQUIREMENTS

Organisations must take active measures to ensure the security of the personal information it holds. This means that an organisation that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

In addition, organisations must actively consider whether it is permitted to retain personal information and should take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the Privacy Act. Importantly, this requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court / tribunal order to retain the personal information.

BREACH NOTIFICATION

Where an "eligible data breach" occurs, the organisation must notify the OAIC and the individuals affected. An "eligible data breach" occurs when:

a. unauthorised access, disclosure or loss (in circumstances where access / disclosure is likely to occur) of personal information;

b. reasonable person would conclude that the access / disclosure (or in the case of loss, potential access or disclosure) would be likely to result in serious harm to any individual to whom the information relates; and

c. the organisation has not been able to prevent the likely risk of serious harm with remedial action (noting that notification to individuals does not constitute remedial action for the purposes of the Privacy Act).

If an organisation suspects that it may have experienced an eligible data breach, it must reasonably and expeditiously assess whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach and take all reasonable steps to ensure the assessment is completed within 30 calendar days of it being aware of the potential eligible data breach. As soon as an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, it must promptly notify affected individuals and the OAIC about the breach. As outlined in the "Enforcement" section below, certain fines will be imposed for "serious or repeated" breaches.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

There is no specific "right to erasure" under the Privacy Act. However, organisations must take reasonable steps to destroy or de-identify the information if it is no longer needed for any purpose permitted under the Privacy Act.

One of the overarching principles of the Privacy Act is that organisations only collect personal information that is reasonably necessary for one or more of its functions or activities, effectively embedding a requirement to minimise the collection and storage of information.

Right to access / correction

On request, organisations must give an individual access to their information and take reasonable steps to correct personal information to ensure that it is accurate, up-to-date, complete, relevant, and not misleading.

Direct right of action

Individuals do not currently have a "direct right of action" for a breach or interference of privacy in Australia. However, individuals may lodge a complaint with the OAIC regarding the handling of their personal information by an organisation if they have first lodged a complaint with the relevant organisation and 30 days have passed since the complaint was lodged and no response has been received. As noted in the "Upcoming reforms" section below, it has been proposed that individuals should have a "direct" right of action against organisations who mishandle their personal information.

PRIVACY BY DESIGN AND DEFAULT

The Privacy Act does not refer specifically to the concept of "privacy by design and default" but it does include various accountability and governance principles. For example, organisations are required to "take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs (and any applicable registered APP code) and to enable complaints". The OAIC's "Privacy Management Framework: Enabling Compliance and Encouraging Good Practice" guidance also places similar focus on strong privacy governance and sets out the OAIC's expectations on steps organisations should take in order to meet this ongoing obligation.

As a result of these ongoing privacy governance obligations, organisations should aim to embed good privacy practices into any design specifications of technologies, business practices and physical infrastructures of the organisation (in effect, privacy by design and default).

In addition, organisations are encouraged to manage privacy risks proactively rather than take a "reactive" approach to addressing any privacy risks that are identified. This requires an understanding of the potential "privacy impacts" of a particular project before the project commences / is deployed. For this reason, organisations are encouraged to undertake privacy impact assessment (**PIAs**). In its simplest form, a PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating those impacts. In Australia, the *Privacy (Government Agencies — Governance) APP Code 2017* requires

Australian Government agencies that are subject to the Privacy Act to conduct PIAs for "high privacy risk projects", namely projects that involve new or changed ways of handling personal information and are likely to have a significant impact on the privacy of individuals.

As noted above in the section "Data Protection Officer (DPO) Requirement", organisations are encouraged to embed a culture of privacy by appointing key roles and responsibilities for privacy management, including a senior member of staff with overall accountability.

ENFORCEMENT

From an enforcement perspective, the OAIC has the power to investigate organisations, request information regarding compliance where there has been a data breach, accept enforceable undertakings, make determinations, issue infringement notices, share information with other enforcement bodies, publish information, and apply to the court for injunctions or civil penalties.

It should also be noted that as part of the 2023 / 2024 Budget, the Federal Government has allocated $45.2 million over four years to the OAIC. This will enhance the resourcing for the OAIC to enforce compliance with the Privacy Act and the Notifiable Data Breaches Scheme, as well as contribute to privacy law reform and the strengthening of protections for personal information.

Currently, civil penalties for "serious or repeated interference with privacy" can be up to a maximum of AUD 2.5 million for individuals. For corporations, it is the greater of:

a. AUD 50 million;

b. 3 times the value of the benefits obtained, if it is quantifiable; or

c. where the benefit cannot be determined, 30% of the corporations 'adjusted turnover' during the 'breach turnover period'.

Although there are no specific penalties applicable to breaches or non-compliance of "data sovereignty or data localisation" requirements, if a breach of an organisation's obligations with respect to cross-border transfers constitutes a "serious or repeated interference with privacy", the OAIC may seek a civil penalty order against that organisation.

Directors' duties

There are no specific directors' duties that apply under the Privacy Act. However, there are general directors' duties under the *Corporations Act 2001* (Cth) that may apply to data protection and security, including the duty to act in good faith in the best interests of the company and to act with reasonable care and diligence.

UPCOMING REFORM

The Privacy Act is expected to undergo major reform in the next 12 months. On 28 September 2023, the Government released its response to the Privacy Act Review Report, setting out an indicative pathway for privacy reforms in Australia. Of the 116 proposals in the Privacy Act Review Report, the Government response agreed to 38 proposals, agreed in-principle to 68 proposals and noted 10 proposals.

Some of the key proposals of reform to which the Government has accepted (or agreed) include:

- ***Overseas data flows:*** introducing a mechanism to prescribe countries and certification schemes that provide substantially similar protection to the APPs;
- ***De-identification:*** further consultation will be required on the proposed introduction of a criminal offence for malicious re-identification where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions;
- ***High privacy risk activities:*** adopting enhanced risk assessment requirements for facial recognition technology and other uses of biometric information as part of implementing requirement to conduct PIAs for high privacy risk activities;
- ***Children:*** defining a child as an individual below 18 years of age and introducing a Children's Online Privacy Code that applies to online services that are "likely to be accessed by children";
- ***Automated decision-making:*** requiring privacy policies to set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's right, and introducing a right for individuals to request meaningful information about how these automated decisions are made;
- ***Security:*** enhancing OAIC guidance on what reasonable steps are to secure, as well as destroy or de-identify, personal information;
- ***Enforcement:*** creating tiers of civil penalty provisions relating to an interference with privacy, giving courts the power to make orders it sees fit after a civil penalty, conferring new powers on the OAIC, and relaxing the threshold for breaches of privacy by eliminating the requirements that breaches need to be repeated.

Some of the key proposals to which the Government *agreed-in-principle* include:

- ***Definitions:*** changes to broaden the scope of the definitions of "personal information" to be information that relates to an individual, "collection" to expressly cover information obtained from any source and by any means and "consent" to be voluntary, informed, current, specific and unambiguous;
- ***Exemptions:*** changes to the current exemptions to certain requirements of the Privacy Act, including the removal of the small business exemption;
- ***Controllers and processors:*** introducing the concepts of APP entity controllers and APP entity processors. Pending the proposal to remove the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Privacy Act in relation to its handling of personal information for that APP entity controller.
- ***Data privacy officer:*** setting out requirements to appoint or designate a senior employee responsible for privacy;
- ***Purposes of processing:*** requiring organisations to determine and record the purposes for which personal information will be collected, used and disclosed, including any secondary purpose;
- ***Fair and reasonable personal information handling:*** a new *'fair and reasonable'* test underpinning the handling of personal information with a list of matters that may be taken into account;

- ***Children:*** additional requirements for personal information of children, including introducing a requirement that collection notices and privacy policies addressed specifically to a child to be clear and understandable, and that children's interest is considered when assessing whether information processing is 'fair and reasonable';
- ***PIAs for activities with high privacy risks:*** requirement to conduct PIAs for activities with high privacy risks prior to commencement of the activities;
- ***Consent:*** increased obligations around transparency and consent, such as expressly recognising the ability to withdraw consent;
- ***Employee records:*** providing additional privacy protections to private sector employees;
- ***Individual rights:*** introducing new rights for individuals to access and to obtain explanations on their personal information, object to the collection, use or disclosure of their information, to opt-out of their personal information being used or disclosed for direct marketing purposes, to request the erasure of that information in certain circumstances, to correct generally available publications and de-index online search results;
- ***Marketing:*** introducing marketing related definitions (i.e. direct marketing, targeting and trading), enhancing safeguards for children in marketing practices, requiring entities to provide information about targeting (incl. information about the use of algorithms and profiling to recommend content to individuals);
- ***Retention:*** introducing the requirement to establish maximum and minimum retention periods in relation to the personal information and specify retention periods in privacy policies;
- ***Data breach notification:*** a new 72-hour window to report eligible data breaches to the OAIC, starting from when they become aware that there are reasonable grounds to believe an eligible data breach has occurred; and
- ***Direct right of action and statutory tort:*** introduction of a direct right of actions for individuals to apply to courts for relief and a statutory tort for serious invasions of privacy.

The Government has also agreed in principle the following proposals relevant to the cross-border disclosure of personal information:

- introducing standard contractual clauses for use when transferring personal information overseas;
- strengthening the informed consent exception by requiring organisations to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent; and
- strengthening transparency requirements relating to overseas disclosures (by requiring organisations, when specifying the countries in which recipients are likely to be located, to also specify the types of personal information that may be disclosed to recipients located overseas).

The Attorney-General's Department will lead the next stage of the reform work, which will involve the drafting and development of legislative amendments informed by a detailed impact analysis and targeted consultations with stakeholders. The Government has indicated that it is committed to introducing draft legislation in 2024.

In December 2022, the Government also released the 2023-2030 Australian Cyber Security Strategy which suggests setting a national framework to respond to major cyber incidents, among other actions. New criminal offences and sanctions laws, including the mandatory reporting of ransomware incidents to the Australian Government, have also been touted as part of the Australian Government's Ransomware Action Plan. The privacy reforms will complement other reforms underway, including Digital ID, the 2023 2030 Australian Cyber Security Strategy, the National Strategy for Identity Resilience, and Supporting Responsible AI in Australia.

PEOPLE'S REPUBLIC OF CHINA

KEY PRIVACY / DATA PROTECTION LAWS

The three "pillars" of China's data protection framework

The People's Republic of China (**China**) has a complex and comprehensive framework of data protection laws. There are three main components to China's data privacy and cyber security regulation: the Personal Information Protection Law (**PIPL**); the Cybersecurity Law of the People's Republic of China (**CSL**); and the Data Security Law of the People's Republic of China (**DSL**).

The CSL was China's first comprehensive national law to address cyber security and data privacy. The CSL sets out a high-level framework to regulate the collection, storage, transmission and use of personal information by Chinese "network operators" and critical information infrastructure (**CII**) operators.

The DSL followed and focuses on protecting national security and covers data security across multiple categories of data (covering more than just personal information).

The PIPL is the most significant data privacy law to be enacted. It is the first comprehensive national law that governs personal information protection in China and complements / clarifies the CSL and DSL. The PIPL applies to any processing activity of the personal information of natural persons in China, regardless of whether the processor is incorporated in China or whether the individual is a Chinese citizen or foreigner located in China.

China also has other data privacy and cyber security obligations enforced in regulations guidelines, codes, decisions, and measures. These include:

- *Civil Code of the People's Republic of China* (**Civil Code**) which codifies an individual's right to privacy, alongside other fundamental human rights, and sets out principles for the protection of personal information in China. The data privacy provisions under the Civil Code are largely aligned with the CSL;
- *Tort Law* which also sets out an individual's right to privacy;
- *Measures on Security Assessment of Cross-border Data Transfer* governing the security assessment process for outbound personal data transfer, effective 1 September 2022;
- *Guidelines for Security Assessment of Cross-border Data Transfer* governing the security assessment process for outbound personal data transfer, August 31, 2022;
- *Implementation Rules for Personal Information Protection Certification* which are guidelines for the certification of personal information protection;
- *Specifications for Security Certification of Cross-border Processing of Personal Information (V2.0–202212)* which are standards for the certification of outbound personal data transfer;
- *Measures for the Standard Contract for Outbound Cross-Border Transfer of Personal Information*, effect from June 1, 2023, which are measures for the Chinese standard contract for outbound personal data transfer; and
- *Guidelines for Filing the Standard Contract for Outbound Cross-Border Transfer of Personal Information*, effective from 30 May 2023, which are guidelines for the Chinese standard contract for outbound personal data transfer.

There are also a range of national standards that provide best practice recommendations in regards to the processing of personal information, such as the *Personal Information Security Standards* and the *Guidance for Personal Information Security Impact Assessment*.

Scope and interaction between the various data protection laws

The CSL, DSL, PIPL, and Civil Code govern data protection from different perspectives:

- the Civil Code sets out some high-level principles and requirements in regard to the processing of personal information;
- the CSL, being China's first comprehensive national law to address cyber security and data privacy, is formulated in the context of cybersecurity. The CSL lays emphasis on cybersecurity, but also contains a chapter on data privacy; and
- the DSL and the PIPL came into force around the same time and developed China's data protection legislation to reflect the evolving data practices in China. The DSL and PIPL address data security from different angles. The DSL emphasises the security of data in the national security sphere, proposing to establish the data management regime (data classification and data categorisation), promoting the utilisation of data and incorporating the data security into national security. The PIPL, on the other hand, is more focused on the protection of personal information. The PIPL sets out detailed requirements for the processing of personal information, including the legal basis, sensitive personal information rules and individuals' rights, etc.

As set out below, "personal information" is defined by the Civil Code, CSL and PIPL, and is generally interpreted to have the similar meaning.

Personal and sensitive personal information

Under the PIPL, "personal information" means *"all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including anonymised information*". This definition clarifies the CSL and confirms that the PIPL does not apply to anonymised information.

The Civil Code, CSL, certain judicial interpretations and sector-specific regulations also each define "personal information". For example, the Civil Code defines personal information to be *"information, recorded electronically or otherwise, that can alone or combined with other information, identify an individual*". To provide some examples, this broad definition would encompass an individual's name, address, birth, ID number, date of birth, biometric information, or health information.

Another example is provided by the Interpretation of *Supreme People's Court and Supreme People's Procuratorate on Several Issues regarding Application of Law in Handling of Criminal Cases Involving Infringement of Citizen's Personal Information* (May 8, 2017) (Interpretation) which defines the "citizen's personal information" for the purposes of the criminal law. The definition under this Interpretation is very similar to the definition in the Civil Code, but includes information that can reflect the activities of particular natural persons.

To provide a final example, under the *Several Provisions on Automotive Data Security Management (for Trial Implementation)* (October 1, 2021), "personal information" refers to all kinds of information related to the identified or identifiable vehicle owners, drivers, passengers, and persons outside vehicles recorded by electronic or other means, excluding the information that has been anonymised.

"Sensitive personal information" is defined in the PIPL to mean *"personal information that, once leaked or illegally used, can easily lead to the infringement of personal dignity of natural persons or the harm on personal and property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts, and other information, as well as the personal information of minors under the age of 14"*. Whilst other definitions of "sensitive personal information" exist in other subsidiary regulations in PRC, the PIPL definition is widely regarded to be the prevailing definition.

Data generated from tracking employees' online activities or prospective customers browsing company websites can be considered sensitive personal information. Internet identity information, e.g. system account number, email address, passwords, passphrases, password protection answers, user personal digital certificates, etc. is also deemed sensitive personal information (reference: Personal Information Security Standards).

REGULATOR / AUTHORITY

Prior to the introduction of the PIPL, there was no single authority responsible for monitoring and enforcing data privacy and cyber security laws in China, but a collection of bodies including the Cyberspace Administration of China (**CAC**), the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration of Market Regulation.

Following the introduction of the PIPL, the CAC is the main body with responsibility for regulating and supervising the protection of personal information in China.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

China is a country that requires local data protection officers. Where the processing of personal information reaches a prescribed threshold under the PIPL, the relevant "personal information processor" (defined as any organisation with discretion to determine the purpose and method of data processing, PIP) must appoint a DPO to supervise the data processing and the protection measures in place. The name and contact details of the DPO must be provided to the CAC. At the time of publication, the processing / volume threshold to trigger the need to appoint a DPO had not yet been made available by the CAC.

However, the *Personal Information Security Specification* which is a recommendatory national standard and therefore provides for best practice recommendations, states that an organisation should establish a full-time DPO position and a department dedicated to the protection of personal information if any of the following conditions are met:

- the main business of the organisation involves the processing of personal information and, the number of employees exceeds 200;
- the organisation processes personal information of more than 1 million individuals, or is estimated to process personal information of more than 1 million individuals during a 12 month period; or
- the organisation processes sensitive personal information of more than 100,000 individuals.

The PIPL requires foreign companies without a presence in China whose data processing activities are subject to the PIPL to set up a dedicated entity or appoint a representative in China to deal with data protection matters.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

If an organisation processes personal information originating from China to provide a product or service to Chinese residents or to analyse their behaviour, it is likely the PIPL will apply. This is the case even if an organisation does not have a physical presence in China. The PIPL has extra-territorial effect and governs the processing of personal information *outside* of China where the purpose of processing is for:

- providing products or services to natural persons in China;
- analysing / assessing the behaviour of natural persons in China; or
- any other circumstances set out in law or regulations.

As described above, foreign companies whose data processing activities are subject to the PIPL will be required to set up a dedicated entity or appoint a representative in China to deal with data protection matters.

EMPLOYEE DATA / INFORMATION

Employee personal data are, by and large, treated similar to other personal data, but they may be collected by PIPs without consent. However, this carve-out from the consent requirement does not apply to the collection of information on job application forms from job applicants or outbound transfer from China of employees' personal information. In these circumstances, employers need to obtain separate consents in addition to complying with other requirements (such as outbound data transfer requirements if the information is going to be shared with parties outside of China).

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Restrictions apply to the transfer of data outside of China. In essence, the cross-border transfer of personal information or important data will be subject to certain restrictions, depending on whether the PIP is a critical information infrastructure operator and the category of data to be transferred out of China.

Specifically under the PIPL, where a PIP needs to provide information to a recipient outside of China (including to a related body corporate), it must meet one of the following compliance steps:

- passing a "CAC Security Assessment" (if applicable);
- obtaining a "personal information protection certification "from a specialist institution in accordance with applicable CAC regulations;
- entering into the template CAC standard contractual clauses with the overseas recipient; or
- meeting any other conditions set by the CAC, or that apply under other laws or administrative regulations.

The CAC and the Innovation, Technology and Industry Bureau of the Hong Kong Special Administrative Region Government (**HKITIB**) signed the Memorandum of Understanding to Facilitating Cross-boundary Data Flow Within the Guangdong-Hong Kong-Macau Greater Bay Area (**MOU**) on 29 June 2023. The details of the MOU itself have yet to be released, however it is anticipated that the MOU will greatly reduce the challenges of managing cross-boundary transfers of personal data within the Greater Bay Area.

PIPs must also obtain the separate consent of the individual to the transfer. The PIPL requires that, in doing so, the PIP notifies the individual of the following information in relation to the transfer:

- the name and contact information of the overseas recipient;
- the purpose and method of the processing;
- the type of personal information involved; and
- how the individual may exercise their rights under the PIPL.

PIPs must also conduct cross-border data transfer assessments. personal information impact assessments (**PIIAs**).

CAC security assessment

Critical information infrastructure operators and PIPs who process personal information meeting a threshold prescribed by the CAC, must domestically store personal information that is collected / generated in China.

Where it is necessary for this personal information to be provided to a recipient outside of China, the critical information infrastructure operator or relevant PIP must pass a security assessment (unless laws, administrative regulations, or CAC rules state that an assessment does not need to be completed).

The Measures on Security Assessment of Cross-border Data Transfer and the Guidelines for Security Assessment of Cross-border Data Transfer governing the security assessment process for outbound personal data transfer sets out that requires the completion of a CAC security assessment must be completed prior to the following types of outbound personal data transfers:

1. A CII operator transfers personal data outside of China;
2. A PIP who processes personal information of one million people or above transfers personal data outside China;
3. A PIP transfers "important data" outside of China ("important data" is defined as data that may endanger national security, economic operation, social stability, public health, and safety once they are tampered with, destroyed, leaked, or illegally obtained or used illegally);
4. A PIP who has cumulatively provided overseas personal information of 100,000 individuals since 1 January of the preceding year transfers personal data outside of China;
5. A PIP who has cumulatively provided overseas sensitive personal information of 10,000 individuals since 1 January of the preceding year transfers personal data outside of China; or
6. Other situations as prescribed by the CAC. No situations has yet been prescribed by CAC.

Personal information protection certification

Certification involves an on-site inspection of the data security capabilities by the certification organisation, and the certification organisation is to monitor the PIP's cross-border data transfer during the validity of the certification.

CAC standard contractual clauses

The CAC standard contractual clauses are provisions to be entered into by data exporters and overseas recipients, governing the rights and liabilities of the parties as well as the individuals. Contracts between

the data exporters and the overseas recipients concerning the cross-border transfer of personal information must not conflict with the CAC standard contractual clauses. In summary:

- the cross-border data transfer of personal information by CIIs and non-CII operators processing of a particular size of data as prescribed by the authorities, will require a CAC Security Assessment;
- the cross-border data transfer of personal information by non-CII operators is generally subject to the requirements of the PIPL; and
- the cross-border data transfer of important data by CIIs and non-CII operators are subject to CAC Security Assessment.

Where treaties or international agreements to which China has concluded or acceded to contain relevant provisions on the cross-border transfer of personal information, then these provisions will still apply.

Do any exceptions apply?

There is no concept of an "adequacy decision" under current Chinese data protection laws, nor any recipient countries that are "exempt", allowing the transfer of personal information without compliance with the above requirements.

However, on 28 September 2023, the CAC issued a public consultation paper on a draft regulation entitled "Regulation to standardise and promote cross-border data flows" (**Draft Regulation**) to streamline the outbound data transfer process.

The consultation paper provides that the Draft Regulation proposes to exempt organisations from the outbound data procedures, including for example, where (a) the amount of personal information to be transferred abroad is less than 10,000 people each year, (b) the outbound transfer of personal information is for contractual necessity (where the individual is a contract party and the transfer is for the purpose of performing under the contract), or (c) the outbound transfer involves employee personal data and the transfer is necessary for the purposes of human resource management. The consultation paper also sets out the Draft Regulation's proposal to allow outbound transfer of personal information of less than 1 million people each year to use the Chinese standard contractual clauses mechanism (easing the requirements to carry out security assessments).

The Draft Regulation is expected to be formally adopted shortly after the end of the consultation period.

Additional protective measures for cross-border transfers

PIPs that transfer information outside of China must adopt necessary measures to ensure that the personal information handling activities of the recipient meet the standard of personal information protection required under the PIPL.

PIPs must also conduct PIIAs prior to transferring personal information outside of China under the PIPL.

The PIIAs will include (as non-exhaustive examples) considering general risks to the data after it is transferred outside of China, national security risks, and the data security and management measures of the recipient.

Data sovereignty / localisation

Data localisation / sovereignty requirements apply in China.

For example, under the PIPL:

- personal information handled by Chinese "state organs" must be stored in mainland China and, if it is necessary for this information to be transferred outside of China, a security assessment must be undertaken; and
- as set out in the "cross-border transfers and data sovereignty" section above, both CII operators and PIPs (or non-critical information infrastructure operators) processing personal information of a particular quantity or threshold (as prescribed by the CAC) must store personal information that is collected / generated in China domestically. Where it is necessary for this personal information to be provided to a recipient outside of China, a security assessment must be completed.

The PIPL also places restrictions on the transfer of personal information to foreign judicial and law enforcement agencies. A PIP must not provide personal information that is stored within China to foreign judicial or law enforcement agencies without the approval of the competent Chinese authority / authorities.

COLLECTION AND PROCESSING OBLIGATIONS

The PIPL sets out a number of legal bases upon which a PIP may collect and process personal information. These are:

- with the consent of the individual;
- where necessary to conclude or fulfill the performance of a contract to which the individual is an interested party, or where necessary to carry out human resources management under an employment policy or collective contracts;
- where necessary to fulfil statutory duties or obligations;
- where necessary to respond to a public health emergency, or for protecting the life, health or property safety of a natural person in the case of an emergency;
- for news reporting or public interest purposes;
- where personal information has been disclosed by the individual or otherwise legally disclosed; or
- for any other circumstance as stipulated by laws or administrative regulations.

Consent is the primary basis for the lawful collection and processing of personal information under the PIPL and must be informed, voluntary and explicit. Individuals may be able to revoke their consent, and a PIP must provide a convenient way for this to occur. Where a PIP changes the purposes of processing, how personal information is processed or the categories of personal information that are processed, consent must be obtained from the individual again.

In comparison, the CSL sets out only one legal base for collecting personal information: individual's consent.

Additionally, where personal information is used for automated decision making about individuals, organisations will need to provide transparent explanations about how decisions are being made and enable individuals to reject the automation and ask for manual reviews.

Sensitive personal information

The collection and processing of sensitive personal information under the PIPL is subject to stricter requirements. To process sensitive personal information, PIPs need to:

- show a specified purpose / purposes for the processing;
- show that the processing of the information is necessary;
- show there are strict measures in place to protect the information;
- undertake a PIIA;
- obtain a separate, express consent to the specific processing activity (as opposed to just general consent); and
- inform the individual why it is necessary for the PIP to process the sensitive personal information and its impact.

Additionally, personal information must not be collected from minors (natural persons under 14 years old) unless separate, explicit consents are obtained from their legal guardian.

Consent

For there to be valid consent, the PIPL requires:

- consent to be given on a voluntary basis, explicit, and given after being fully informed;
- new consents to be obtained where there is any change to the method or purpose of information processing or any change to the type of personal information being processed; and
- individuals to have a right to withdraw consent (with processors required to provide a convenient way to withdraw). In addition, if an individual refuses or withdraws their consent, a processor cannot refuse to provide the products or services to the individual, unless the personal information is necessary for the provision of such products or services.

SECURITY REQUIREMENTS

Security obligations are contained in each of the CSL, DSL and PIPL.

The PIPL requires PIPs to take necessary measures to safeguard the security of the person information they handle and:

- adopt technical security measures such as encryption and de-identification;
- conduct regular security education and training for employees; and
- implement and maintain a personal information security incident response plan.

Data minimisation requirements also apply in China, and this is one of the overarching principles of the PIPL. The processing of personal information must have specified and legitimate purposes, be directly related to the purpose of the processing and be processed in a manner that has the least impact on an individual's personal rights and interests. In addition, a PIP may only collect the minimum amount of personal information that is required to achieve the processing purpose, and collection must not be excessive, effectively embedding a requirement to minimise the handling and storage of personal information.

A PIP is also required to take steps to proactively delete an individual's personal information in a number of situations, including where the purposes of the data processing have been achieved or it is not possible, or is no longer necessary to achieve these purposes.

BREACH NOTIFICATION

Data breach notification requirements are set out in each of the CSL, DSL and PIPL. There are generally stringent timelines to be followed.

Where a personal data breach (being a personal information leak, distortion or loss) occurs or may have occurred, the PIPL requires PIPs to immediately adopt remedial measures and notify the relevant regulator and possibly notify impacted individuals.

The notification to the regulator must include:

- the types of personal information involved in the breach;
- the cause(s) of the data breach incident;
- the possible consequences / impacts;
- the remedial measures taken by the PIP and measures available to individuals to mitigate the damage; and
- the contact details of the PIP.

Where the PIP is successfully able to adopt measures to avoid harm to individuals created by the data breach, the PIP does not have to notify individuals, unless instructed to do so by the regulator.

While the PIPL doesn't provide a specific time frame for notification (only specifying that the notice must be *immediate*) it is possible that future regulations may require that:

- for incidents that create harm to individuals or organisations, a PIP must provide a report to the such individuals or organisations within 3 business days; and
- for incidents involving personal data of more than 100,000 individuals or any "important data", notification should be provided to the CAC or another relevant regulator within 8 hours of the incident. A second report must then be provided to the CAC within 5 business days of the incident being resolved.

In contrast, the CSL provides general requirements on cybersecurity related security incidents and the need to report to the relevant authority of the incident. The DSL also requires the reporting of incidents to the individuals and relevant authorities.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

A PIP must proactively delete an individual's personal information if any one of the following circumstances occur:

- the purposes of the data processing have been achieved or it is either not possible to or is no longer necessary to achieve these purposes;
- the PIP has stopped providing the agreed products or services, or the agreed information retention period has expired;

- the individual rescinds its consent to the processing of its personal information;
- personal information is processed by the PIP in breach of laws, administrative regulations or agreements; or
- any other circumstances provided by laws or administrative regulations.

Where a PIP has not deleted an individual's personal information in the above situations, the individual may request that the PIP do so.

Right to access / correction

Under the PIPL, an individual may request that a PIP corrects or updates their personal information where they discover that it is incorrect or incomplete. A PIP must complete this request in a timely manner.

Individuals also have the right to "know and decide" in relation to the processing of their personal information and generally have the right to consult with and copy their personal information from a PIP. Individuals may also request that data handling rules are explained to them.

Direct right of action

Under the PIPL, individuals have a direct, private cause of action to sue a PIP where the processor has prevented or rejected the individual from exercising its rights.

An individual whose rights in relation to their personal information have been infringed can also seek civil remedies under the *Civil Code* (i.e. for tortious acts that endangers their personal or property safety) and other relevant laws, including the *Consumer Rights Protection Law*. These remedies include requiring the PIP to cease the infringement, remove the obstruction or to remove the danger caused to that individual.

It is also relevant to note that "public interest litigation" may also be brought by representative organisations or bodies on behalf of individuals where the processing activities infringe upon the rights or interests of a significant number of individuals.

In addition, pursuant to the *Provisions of the Supreme People's Court* on *Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies to Process Personal Information,* where the individual requests the PIP to delete facial information together with a claim for the liability of breach of contract, the court shall uphold such request. If the PIP defends itself on the ground that both parties fail to make an agreement on the deletion of facial information, the court shall not uphold such defence.

PRIVACY BY DESIGN AND DEFAULT

The principles / objectives of "Privacy by Design" and "Privacy by Default" are enshrined in many aspects of the PIPL. For example, under the PIPL, various measures must be adopted by a PIP to ensure that personal information is processed in compliance with law and to prevent data breaches. Such measures include:

- formulating internal management structures and operating rules;
- implementing categorised management of personal information; and
- determining reasonable operational limits for personal information and regularly conducting security education and training for employees.

In addition, the PIPL specifies the obligations of important internet platform service providers, such as establishing a sound personal information protection policy and system, developing platform rules and publishing a social responsibility report on personal information protection on a regular basis.

As noted above in the section "Data Protection Officer (DPO) Requirements", organisations are required to appoint a DPO, helping to embed a culture of privacy and privacy management in organisations.

ENFORCEMENT

Enforcement powers, actions, and penalties for non-compliance with privacy and data protection laws in China depend on the specific law or regulation that is breached. The PIPL does not stipulate a single supervisory authority that is responsible for personal information protection matters.

Under the PIPL, the relevant regulatory authorities have the following enforcement / investigative powers:

- interviewing relevant parties, and investigating personal information processing activities;
- review / taking copies of relevant materials related to personal information processing activities;
- conducting on-site inspections and investigating personal information processing activities that are suspected to be unlawful; and
- inspecting (and possibly sealing and confiscating) the equipment and articles relevant to personal information processing activities.

Organisations and individuals may be subject to the following penalties or enforcement action where they are processing personal information in violation of the PIPL, or otherwise breach obligations under the law:

- an order to rectify breaches;
- warnings;
- confiscation of unlawful gains or income;
- an order to suspend / terminate the provision of apps that are unlawfully processing personal information;
- an order to suspend business activities or relevant licenses / permits; and
- in respect of a responsible individual, prohibiting that person from holding the position of director, supervisor, senior manager, or personal information protection officer for a certain period of time.

In terms of possible fines, an organisation can be subject to a financial penalty of up to RMB 50 million or 5% of the organisation's revenue in the previous year for non-compliance. An individual directly liable for the violations of the PIPL can also be personally fined up to RMB 1 million, subject to disciplinary actions and even prison.

Violations of the PIPL can be recorded in an organisation's credit file and made public (which therefore threatens access to credit and the purchase of property, as well as reputational damage) and criminal sanctions are possible where a relevant criminal law has been violated. There are no caps for civil liability cases.

Consequences for breaches of data sovereignty / data localisation requirements

There are no specific consequences attached to breach / non-compliance with the data localisation / sovereignty requirements under the PIPL. Instead, a breach of these provisions would fall under the general legal liability provisions of the PIPL which provide that anyone processing personal information in violation of the law or who fails to perform an obligation can be subject to the enforcement measures we have described below, or the fines / penalties set out above.

Directors' duties

The PIPL does not place specific duties on directors and / or officers per se. However, as set out above, a penalty may be imposed on an individual if he / she is directly liable for breaches of the PIPL. There are no obligations of directors or officers under PRC corporate laws that are specially related to privacy or data protection. However, in some industries, for example, for banking and financial entities, the senior management or person in charge may be exposed to sanctions personally if the PIP violates data privacy and / or cybersecurity rules.

UPCOMING REFORM

The data protection framework in China is still evolving, with new regulations, guidance documents and measures expected to be released to assist in interpretation and application of this framework. These recent regulatory developments mean that it is important for organisations to monitor for changes to this framework, including by considering the release of any draft or final regulations, guidance documents or measures.

Significant reforms include:

- amendment to the CSL which will increase the amount of penalties;
- data breaches reporting deadlines (for data breaches that create harm to individuals or organisations, a PIP must provide a report to such individuals or organisations within 3 business days, and for data breaches that relate to "important data" or that impact more than 100,000 people, notification should be made to relevant authorities within 8 hours and a full report should be sent to CAC within 5 business days after handling the data breach); and
- detailed, practical guidelines on CIIs and "important data".

HONG KONG

KEY PRIVACY / DATA PROTECTION LAWS

The main data protection law in Hong Kong is the *Personal Data (Privacy) Ordinance — Cap 486* (**PDPO**). The PDPO sets out obligations in relation to the collection and handling of personal data by the private and public sectors, including the 6 Data Protection Principles (**DPPs**).

REGULATOR / AUTHORITY

The Office of the Privacy Commissioner for Personal Data, Hong Kong (**PCPD**) is the government agency responsible for administering the PDPO.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

There is no formal requirement to appoint a data protection officer. However, DPP requires organisations to publish the contact details of individuals within the organisation who will handle requests and queries from individuals.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The PDPO obligations apply to the handling of "personal data" which is defined as any data:

a. relating directly or indirectly to a living individual;

b. from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

c. in a form in which access to or processing of the data is practicable.

"Data" includes personal identifiers assigned to users, such as IP addresses.

There is no express concept of "sensitive" personal data in the PDPO, but the PCPD has published Codes of Practice / Guidelines providing additional guidance on the use of:

- HKID numbers;
- Biometric data (for example, DNA samples);
- human resources management;
- consumer credit; and
- employee monitoring.

Extra-territorial application

The PDPO applies to "data users" who control the processing of personal data in or from Hong Kong. There is no express extra-territorial application, though foreign organisations that operate in Hong Kong are required to comply.

There is also no specific registration requirement for organisations that collect and handle personal data in Hong Kong. However, there is a provision that enables the PCPD to impose registration and reporting obligations on certain classes of organisations (although none have been imposed to date).

EMPLOYEE DATA / INFORMATION

The PDPO regulates employee data in the same way it regulates personal data collected and processed outside the employment context. There are no specific requirements for obtaining employee consent.

Consistent with the PDPO requirements pertaining to personal data, on or before the collection of personal data from an employee, an employer should provide the employee with a notice statement, informing the employee about the purposes for which the data will be used, the classes of persons to whom the data may be transferred, the rights of the employee to make data access and correction requests, and the contact details of the person to whom the employee can make such request.

An employer should not disclose employment-related data of employees to a third party (including those located overseas) without first obtaining the employees' express and voluntary consent, unless the disclosure is for purposes directly related to the employment or such disclosure is required by law.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Although the PDPO contains proposed restrictions in relation to cross-border transfers, these have not come into effect and are not expected to come into effect in their current form. As a result, there are currently no express restrictions in the PDPO on cross-border transfers.

However, the DPPs are applicable to all transfers of personal data and will apply to cross-border transfers. In particular, the DPP contains requirements that individuals be informed of the classes of people to whom their personal data may be transferred, and that uses of personal data (including transfers) must either:

a. fall within the original purpose for which the personal data was collected (or a directly related secondary purpose);

b. be done with the reasonable belief that the use of the data for a new purpose is "clearly in the interest" of the individual; or

c. be done with the individual's consent.

Special rules apply to cross-border transfers of personal data from mainland China to Hong Kong. The Cyberspace Administration of China (**CAC**) and the Innovation, Technology and Industry Bureau of the Hong Kong Special Administrative Region Government (**HKITIB**) signed the Memorandum of Understanding to Facilitating Cross-boundary Data Flow Within the Guangdong-Hong Kong-Macau Greater Bay Area (**MOU**) on 29 June 2023. The details of the MOU itself have yet to be released, however it is anticipated that the MOU will greatly reduce the challenges of managing cross-boundary transfers of personal data between the Greater Bay Area.

Additional protective measures for cross-border transfers

As set out above, there are no specific protective measures that must be taken for cross-border transfers. The PCPD has published "model clauses" as part of its guidance on cross-border transfers, but as the proposed restrictions in the PDPO has not come into effect, organisations are not yet required to implement the model clauses.

However, general obligations applying to all transfers of personal data will still apply to cross-border transfers. These include the obligations to have appropriate contractual measures in place when engaging data processors.

Data sovereignty / localisation

The PDPO does not contain any specific data sovereignty or localisation requirements (such as governmental consent, approval, or registration requirements).

COLLECTION AND PROCESSING OBLIGATIONS

Collection

Any collection of personal data must be:

a. done for a lawful purpose directly related to a function or activity of the data user;

b. necessary for or directly related to that purpose; and

c. adequate but not excessive in relation to that purpose.

The collector of this data is referred to as a "data user".

In addition, personal data must only be collected by means which are "fair in the circumstances", and after having been provided with information about:

a. whether it is obligatory or voluntary to provide the data;

b. the purposes for which the data will be used;

c. the classes of persons to whom data may be transferred; and

d. individual rights to access and correct the data (including the contact details of the person to whom such requests are to be made).

Processing

The processing of personal data must either:

a. fall within the original purpose for which the personal data was collected (or a directly related secondary purpose);

b. be done with the reasonable belief that the use of the data for a new purpose is "clearly in the interest" of the individual; or

c. be done with the individual's consent.

Consent

In general, consent may be implied such as by sending an email to the individual and assuming his / her consent, if the individual does not reject the consent in a certain period. There are two exceptions:

a. if a new purpose is involved — in which case, express consent of the individual given voluntarily is needed; or

b. if direct marketing is involved — in which case, it will not be possible to rely on implied consent. Consent for direct marketing cannot be inferred from the individual's non-response. Consent must be explicit. A failure to obtain consent constitutes an offence in Hong Kong.

Consent must be given voluntarily and may be withdrawn at any time.

SECURITY REQUIREMENTS

An organisation must take "all practicable steps" to ensure that personal data is protected against unauthorised loss or access. This includes the implementation of appropriate contractual measures to prevent unauthorised access or loss or use of the data transferred to a data processor.

Data minimisation

Organisations are to only collect personal data that is "necessary" and "not excessive" to achieve a particular purpose. Personal data must only be kept for no longer than is necessary.

Whilst there are no specific security or data minimisation obligations in relation to cross-border data transfers, organisations need to consider the following factors in determining whether measures taken are "practicable" to protect personal data, including the "physical location where the data is stored".

BREACH NOTIFICATION

There is no mandatory breach notification requirement. However, the PCPD encourages voluntary notification of data breaches to the PCPD and / or affected individuals.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

There is no specific "right to erasure" or "right to be forgotten" under the PDPO. However, organisations are required to not keep data for longer than is necessary to fulfil the purpose for which it is used.

Right to access / correction

Individuals have a right to request access to the personal data that an organisation holds about them. The request must be answered by the organisation "within a reasonable time" and "in a reasonable manner" and in a form that is intelligible. Individuals may also lodge a formal "data access request" to receive a copy of any personal data the organisation holds about them.

Individuals may also request the correction of that personal data and lodge a formal "data correction request" which must be complied with within 40 days.

Direct right of action

Individuals who suffer damage (including "injury to feelings") as a result of a contravention of the PDPO by an organisation can bring a civil action to claim compensation. The PCPD may provide some legal assistance to the individual if it believes it warrants intervention. An individual can also complain to the PCPD who may then either carry out, refuse to carry out or terminate the investigation of the complaint.

PRIVACY BY DESIGN AND DEFAULT

There is no explicit requirement to implement privacy by design. However, the PCPD has published a *"Guide to Data Protection by Design for ICT Systems"* jointly with the Singaporean Personal Data Protection Commissioner. Although this guidance is not tied to PDPO obligations, it recommends that organisations be "proactive" in identifying data risks; not collect more data than is necessary; and implement "end-to-end" security across the software development lifecycle.

ENFORCEMENT

The PCPD has powers to investigate complaints it receives about alleged breaches of the PDPO, or to commence investigations on its own initiative. For the purposes of the investigation, the Commissioner may summon people to give evidence and inspect personal data systems.

The PCPD may issue an "enforcement notice" if its investigation reveals breaches of the PDPO. The enforcement notice may direct an organisation to remedy and prevent recurrences of the breaches, and failure to comply with the enforcement notice is an offence the penalty for which is a fine of HKD 50,000, imprisonment for 2 years, and a daily penalty of HKD 1,000 per day.

The PDPO also stipulates a range of other specific penalties, such as a fine of HKD 1,000,000 or 5 years' imprisonment for disclosure of personal data without consent, with an intent to obtain gain in money or other property (or an intent to cause loss in money or other property to the individual).

UPCOMING REFORM

The Hong Kong government is amending the law and the reforms would likely include the introduction of:

- a mandatory data breach reporting regime;
- a requirement for organisations to have an express data retention policy;
- the direct regulation of data processors;
- requirements relating to cross-border transfer of personal data; and
- increased administrative fines for breaches of the PDPO.

These reforms are expected to occur within the next year and prior to 2025.

INDIA

KEY PRIVACY / DATA PROTECTION LAWS

The Information Technology Act 2000 (**IT Act**) is currently the primary source of data protection law in India. The IT Act incorporates rules, namely the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (**Rules**) and the *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013,* which provides practices and procedures to be adopted by an organisation in order to secure its data.

The IT Act and Rules govern the collection, processing, use and storing of "personal information" by people and bodies corporate in India. "Personal information" is defined in the Rules to mean "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person".

There are also some industry-specific regulations that contain some related data protection obligations, for example, healthcare and financial services.

On 11 August 2023, the Digital Personal Data Protection Act, 2023 (**DPDP Act**) was passed by the Indian Parliament. The DPDP Act will be India's first comprehensive set of data protection laws. The specific rules under the DPDP Act are yet to be formulated.

The date in which the DPDP Act will be brought into effect is yet to be notified, with different sections of the legislation set to come into force at different times. Once in force, the DPDP Act will replace section 43A of the IT Act (which lays down the penalties on body corporates for failure to protect sensitive personal data) and the Rules.

REGULATOR / AUTHORITY

Currently, the Ministry of Electronics and Information Technology (**Ministry**) administers the IT Act. There is no dedicated authority responsible for overseeing privacy or data protection in India.

When the DPDP Act comes into force, the Central Government will establish the Data Protection Board, which will administer the DPDP Act.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

There is no current requirement under the IT Act to appoint a DPO. However, organisations need to designate and publish the contact details of a "grievance officer" who is responsible for addressing complaints from individuals.

With the enactment of the DPDP Act, every "significant data fiduciary" (being any data fiduciary that the Central Government assesses as being a significant data fiduciary on the basis of various factors (e.g. the volume and sensitivity of personal data processed, risk to individuals' rights, potential impact on

sovereignty and integrity of India, etc.) is required to appoint a DPO for addressing the concerns and questions of "data principals" — those individuals whose data is collected and processed. The DPO will represent the significant data fiduciary under the DPDP Act, and will answer to the organisation's board (or similar governing body). The DPO must be based in India.

However, every "data fiduciary" (i.e. a data controller) must appoint a "grievance officer" to act as the point of contact for individuals who wish to raise issues with the data fiduciary.

The contact details for both DPOs and grievance officers must be published.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The IT Act regulates the handling of "personal information" by companies.

As detailed below, additional obligations apply to "sensitive personal information", which is defined in the Rules as personal information relating to:

a. passwords;

b. financial information such as bank account or credit card details;

c. physical, physiological and mental health condition;

d. sexual orientation;

e. medical records and history;

f. biometric information or;

g. any detail relating to the above as provided to an organisation for providing the service.

The IT Act has extraterritorial application and applies to both acts within India by Indian companies and to acts committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

The DPDP Act will apply to:

- all digital personal data that is processed within India (whether collected from individuals online or offline but digitised afterwards); and
- all digital personal data processed outside India, if such processing is in connection with any activity related to offering of goods or services within the Indian territory.

The DPDP Act will not apply to:

- personal data processed by an individual for any personal or domestic purpose;
- personal data that is made or caused to be made publicly available by the individual to whom such personal data relates; and
- any person who is under an obligation under any law for the time being in force in India to make any personal data publicly available.

Unlike many other jurisdictions, the DPDP Act gives equal merit of protection to all digital personal data, and does not separately classify any data categorisation as sensitive personal data or critical personal data.

EMPLOYEE DATA / INFORMATION

There are no specific requirements imposed on processing the employees' personal data under the IT Act. Under the DPDP Act, an employer will not be required to seek employee consent for processing of the employee's personal data if:

- such processing is for employment related activities (such as providing employee benefits, payroll processing, medical purpose, etc.); or
- such processing is to protect itself from loss or liability (such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, etc.).

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Currently under the IT Act, there are no specific requirements imposed on the transfer of data outside India. However, sensitive personal information may only be transferred:

- to any other body corporate that ensures the same level of data protection as is required under the Rules; and
- either:
  - the transfer is necessary for the performance of the lawful contract between the body corporate and the data subject; or
  - or the data subject has consented to data transfer.

Under the DPDP Act, personal data can be transferred to any country outside India except to countries restricted by government notifications (blacklisted countries). There are certain exemptions wherein personal data can be transferred to the blacklisted countries, such as for any action which is necessary for enforcing any legal right or claim, for performance of statutory function by court, to effectuate authorised mergers and acquisitions or other schemes of arrangement, etc.

Additional protective measures for cross-border transfers

There are no additional protective measures for cross-border transfers either under the IT Act or the DPDP Act.

Data sovereignty / localisation

Both the IT Act and the DPDP Act do not contain any specific data sovereignty or localisation requirements (e.g. requiring specific categories of information to remain in India). However, there are sector-specific localisation requirements for financial services providers, under which banks and payment service providers must store the data related to the Indian leg of transactions in India.

COLLECTION AND PROCESSING OBLIGATIONS

The Rules currently require organisations to provide a privacy policy setting out details of the collection of personal information, purpose of collection, intended recipients of the personal information.

Sensitive personal information must only be collected if it is necessary for a lawful purpose connected with the functions or activity of the organisation, and only with written consent to that collection. Once collected, sensitive personal information must only be used for the purposes for which it was collected and only disclosed with the data subject's permission. Organisations must only hold sensitive personal information for as long as it is required and may lawfully be used.

Organisations must obtain consent from individuals in writing for the collection, use and transfer of their sensitive personal information. There is no explicit mention of any consent requirements in the IT Rules for personal information. Under the DPDP Act, there are a number of personal data collection and processing obligations:

1. Issuing notice to individuals

If the personal data was collected from individual prior to the DPDP Act coming into force, then notice must be provided to the individual as soon as it is reasonably practicable upon the individual giving consent to process their personal data.

After the enactment of the DPDP Act, notice must be provided to the individual at the time of obtaining consent for data collection.

Certain disclosures are required to be made in the notice:

- personal data being collected and the specific purpose of processing such personal data;
- the rights of individuals granted under this Act and the manner in which such rights can be exercised (such as right to withdrawal of consent, right to grievance redressal, right to access information about personal data, etc.); and
- contact details of the person who will respond to any communication from the individual.

Individuals must be given an option to view the notice in English or in any of the 22 languages specified in the 8th Schedule of the Indian Constitution.

2. Contractual obligations:

Data controllers / data fiduciaries are required to enter into robust valid contracts with the data processor for processing personal data.

3. Additional obligations for processing personal data of children

Data controllers / data fiduciaries must obtain verifiable consent from the child's parent or lawful guardian before processing such child's personal data. In addition, tracking or behavioural monitoring of children or targeted advertising directed at children is not allowed.

There are additional obligations that a significant data fiduciary is required to take in addition to the obligations outlined above:

a. appoint a DPO (as outlined in the DPO Requirement section);

b. appoint an independent data auditor who would carry out periodic audits independently and evaluate the compliances in accordance with the DPDP Act; and

c. undertake periodic data protection impact assessments (**DPIA**) in accordance with the DPDP Act. Such assessment shall comprise of a description of the rights of individuals, purpose of processing their personal data, assessment and management of the risk to the rights of individuals and other matters as prescribed under the DPDP Act.

SECURITY REQUIREMENTS

Both the Rules and the DPDP Act require organisations to keep personal information/personal data secure by implementing appropriate security standards and procedures and maintain documentation for the same which are to be provided to the authorities, if required.

Data minimisation

There are no requirements for data minimisation under the IT Act.

Under the DPDP Act, the data controller / data fiduciary is required to collect only as much personal data as is necessary to serve the purpose for which the individual has given consent.

Further, the data controller / data fiduciary will cause itself as well as its data processor to erase the personal data collected when the specified purpose for which such data was collected has been served or when the individual withdraws his/her consent, whichever is earlier. However, the data controller / data fiduciary shall retain such personal data if it is necessary for complying with any law.

BREACH NOTIFICATION

Under the IT Act, companies need to notify the Indian Computer Emergency Response Team (**Cert-In**) of certain types of real or suspected cyber security incidents (for example, unauthorised access to IT systems and distributed denial of service attacks) which is likely to cause an offence or harm by impairing the confidentiality, integrity or available of electronic information, systems, services, or networks of an organisation. These incidents must be notified within a reasonable time of occurrence or noticing the incident to have scope for timely action.

The DPDP Act stipulates that the data controller / data fiduciary is required to notify all personal data breaches to the Data Protection Board and each affected individual. The timeline for reporting a data breach under the DPDP Act is expected to be clarified by way of rules.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

There is no specific “right to be forgotten” under the IT Act. However, as described above, sensitive personal information must only be kept for as long as it is required.

Similarly, there is no specific "right to be forgotten" under the DPDP Act. However, as described above, personal data must only be kept for as long as it is required or till the individual withdraws consent, unless such personal data retention is necessary under any law.

Right to access / correction

Under both the IT Act and the DPDP Act, on request, organisations must allow an individual to review personal information held about them and, if requested, the organisation must then take steps that are feasible to correct any "deficient" or "inaccurate" personal information.

Direct right of action

Individuals also have a direct right under the IT Act to claim compensation from an organisation where that organisation "is negligent in implementing and maintaining reasonable security practices".

The DPDP Act, however, does not provide the individuals for any direct right to claim compensation whose personal data has been compromised.

PRIVACY BY DESIGN AND DEFAULT

Not applicable.

ENFORCEMENT

Fines and criminal penalties imposed under the IT Act vary for each offence, but can be up to INR 500,000 (approx. USD 6,500) and 3 years' imprisonment for the officers in charge of the organisation.

As mentioned above, aggrieved data subjects are able to seek compensation where an organisation has failed to implement and maintain reasonable security practices.

Fines for non-compliance of the DPDP Act may vary up to INR 250 million (approx. USD 30 million). The DPDP Act does not impose any criminal penalty for non-compliance.

Consequences for breaches of data sovereignty / data localisation requirements

Not applicable.

Directors' duties

Not applicable.

UPCOMING REFORM

The DPDP Act is likely to come into force once the rules under the DPDP Act are finalised and the Data Protection Board of India is set up. As set out above, data controllers / data fiduciaries are likely to be granted a transition period to comply with the provisions of the DPDP Act once notified.

INDONESIA

KEY PRIVACY / DATA PROTECTION LAWS

The fundamental basis of the right of privacy in Indonesia is encompassed in the 1945 Constitution of the Republic of Indonesia, which provides for the right to: (i) self-protection, protection of each data subject's families, respect, dignity and properties under their control; as well as (ii) security and protection from the threat of fear for doing or not doing something, which constitutes human rights.

As of 17 October 2022, Law No. 27 of 2022 on Personal Data Protection (**PDP Law**) came into effect with a transition period of two years for the relevant parties (including personal data controller and personal data processor) to comply with the personal data processing compliance and requirements. The PDP Law is an implementation of the rights established in the 1945 Constitution as referred to above.

Under the PDP Law, a "personal data controller" is defined as any person, public body and international organisation that acts individually or jointly in determining the purpose of data processing and performing control over data processing activities.

"Personal data processor" is defined as any person, public body and international organisation acting individually or jointly in processing personal data on behalf of the personal data controller.

The enactment of the PDP Law is a major progression for the protection of personal data in Indonesia, where the PDP Law serves as the umbrella law for the implementation of personal data protection in Indonesia. The PDP Law is the long-awaited and first comprehensive set of laws in Indonesia to govern personal data protection in both electronic systems and non-electronic systems. In comparison to the previously enacted regulations that govern personal data protection in Indonesia, the PDP Law specifically sets out more robust, clear and strict rules to protect personal data.

In addition to the PDP Law, there are a number of regulations (for example, sectoral regulations and/or regulations which regulate certain matters (e.g., medical records, financial services' consumers data, etc.)) that exist which regulate the handling of personal data of Indonesian citizens by the personal data controller (including electronic systems of electronic system providers that are categorised into electronic system providers in the private sector and the public sector (**ESP**), referred to collectively as the Personal Data Protection Regulations (**PDP Regulations**).

The main PDP Regulations are:

- the PDP Law;
- *Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016* (**EIT Law**);
- *Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions* (**GR 71/2019**);
- Minister of Communications and Informatics (**MOCI**) *Regulation No. 5 of 2020 on Electronic System Provider in the Private Sector as amended by the MOCI Regulation No. 10 of 2021* (**MOCI Reg 5/2020**); and
- *MOCI Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems* (**MOCI Reg 20/2016**).

There are also other related personal data protection regulations that may apply in certain matters or to certain sectors, including:

- *Ministry of Health Regulation No. 24 of 2022 on Medical Record*, which sets out obligations pertaining to the storing, retaining, deletion and confidentiality of medical records;
- *Financial Services Authority Regulation No. 6/POJK.07/2022 on the Consumer and Public Protection in the Financial Services Sector,* which sets out obligations relating to the processing of consumer data by the financial services sector;
- *Central Bank of Indonesia Regulation No. 3 of 2023 regarding Consumer Protection of the Central Bank of Indonesia,* which sets out obligation for entities which are under the supervision of Bank Indonesia to keep the confidentiality and security of its customers' data; and
- *Law No. 36 of 1999 on Telecommunications* (as partially amended by Law No. 6 of 2023 on Stipulation of Government Regulation in Lieu of Law No. 2 of 2022 on Job Creation into Law), which regulates the handling of information transmitted via telecommunication networks or telecommunication services provided by telecommunication operators.

REGULATOR / AUTHORITY

The PDP Law mandates the Indonesian Government to set up a specific Data Protection Authority (*Lembaga*) that is responsible for upholding the rights of data subjects to the protection of their personal data. The Data Protection Authority is also responsible for the enforcement and monitoring of compliance of business entities with the PDP Regulations. However, up to the date of release of this publication, the Data Protection Authority is yet to be established.

MOCI, which was established to carry out government affairs in the field of communication and information technology, continues to exercise its authority to impose sanctions in relation to the non-compliance on the data protection related obligations or processing (e.g., based on MOCI Reg 20/2016).

DATA PROTECTION OFFICER (DPO) REQUIREMENT

Under the PDP Law, there is a specific requirement for personal data controllers and personal data processors to appoint an officer to perform the function of protecting personal data in the following circumstances:

a. the processing of the personal data is for the benefit of public services;
b. the nature, scope and/or objectives of the personal data controller require regular and systematic monitoring of personal data on a large scale; and
c. the main activities of the personal data controller consist of processing large-scale personal data for specific personal data and/or personal data relating to criminal offences.

The PDP Law allows for the DPO to be internally appointed from within the personal data controller or personal data processor organisation, or recruited externally specifically for the purpose of undertaking the duties of a DPO.

The primary duties of a DPO are to:

- monitor and ensure compliance with the PDP Law and the policy of the personal data controller or the personal data processor;
- provide information and guidance/advice to data controllers or data processors to comply with the provisions of the PDP Law;
- provide advice regarding the personal data protection impact assessment and supervise the performance of personal data controllers and personal data processors; and
- act as the contact person and liaise/coordinate for issues related to personal data processing matters.

The Indonesian Government will look to release a more detailed guidance / regulation documents in relation to DPO duties. Until the date of this publication, the related guidance/regulation only refers to the Decree of Minister of Manpower Number 103 of 2023 on the Stipulation of Indonesian National Competency Standards in the Information and Communication Category of the Subject Matter of Programming Activities, Computer Consultancy and Related Activities in the Expertise Area of Personal Data Protection (**MOM Decree No. 103/2023**) that was recently stipulated. Such MOM Decree No. 103/2023 provides the guidance to determine human resources competency, recruitment needs, training, and certification related to personal data protection.

Aside from the DPO requirements above, MOCI Reg 20/2016 requires ESPs to have a person within the organisation to whom an individual (data owner or currently known as data subject under the PDP Law) can contact in relation to the management of their personal data. MOCI Reg 20/2016 does not explicitly mandate whether the individual appointed as the contact person needs to be an Indonesian citizen or be based in Indonesia. However, there is a general requirement for that person to be easily contactable by the data owner.

SCOPE AND EXTRA TERRITORIAL APPLICATION

The PDP Law applies to every person, public agency and internal organisation that performs legal acts that are:

a. located within the jurisdiction of Indonesia; and

b. located beyond the jurisdiction of Indonesia which has legal consequences:

   i. within the jurisdiction of Indonesia;

   ii. towards the Indonesian data subjects outside the jurisdiction of Indonesia.

The PDP Law broadly defines “personal data” to be “any data of an individual who can be identified and/or may be identified individually or combined with other information both directly or indirectly through electronic or non-electronic systems”. Personal Data is further distinguished into General Personal Data and Specific personal data.

Specific personal data under the PDP Law is referred to as personal data which, if processed, can have a greater impact on the data subject. Specific personal data includes:

- health data and records;
- biometric data;
- genetic data;
- sexual life / orientation;
- political views;
- criminal records;
- children's data;
- personal financial data; and / or
- any other data as provided in accordance with the prevailing laws and regulations (for example, medical record, medical condition and care, treatment of physical and psychological health, etc, based on Law No. 17 of 2023 on Health).

Furthermore, EIT Law expressly applies to Indonesians, foreign data subjects and entities, and to all electronic transactions processed within or outside Indonesia that have legal consequences in Indonesia or result in impacts that are "detrimental to Indonesia's interest" (including but not limited to Indonesia's national economic interests, citizens, the dignity of the nation, state defence and security, state sovereignty and strategic data protection).

In addition, ESPs in the public sector and ESPs in the private sector must register themselves to the MOCI as an ESP before the users can use the ESP, which administrative sanctions may be imposed (e.g., in the forms of written warnings, fines and / or temporary suspension of the ESP) if there are failures to do so.

EMPLOYEE DATA / INFORMATION

The PDP Law, as well as Law No. 13 of 2003 on Manpower (as recently amended by Law No. 6 of 2023 on the Stipulation of Government Regulation No. 2 of 2022 in Lieu of Law No. 11 of 2020 on Job Creation into Law) (**Manpower Law**) does not specifically regulate regarding the protection of employee personal data or information. Employee data is treated the same as personal data under the PDP Law. As such, it follows that the level of protection that is provided towards employee personal data follows the level mandated by the PDP Law.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

During the transitional period of the PDP Law, the other relevant PDP Regulations will apply to the transfer of personal data. The PDP Regulations require data controllers (including ESPs) to obtain informed consent from the data subject and verify the accuracy of the data being collected and used. ESPs are also required to coordinate the transfer with the MOCI by submitting an offshore personal data transfer implementation plan and report (post-completion of the data transfer). The data transfer plan must contain at least the country and the full name of the data recipient as well as the intended date of the data transfer implementation and the background/purpose of the data transfer.

Once the PDP Law is fully in force (i.e., when the transition period ends on 17 October 2024), personal data controllers are permitted to transfer personal data to other personal data controllers and / or personal data processors outside the borders of Indonesia as long as the country of the receiving entity has personal data protections at a level that is equal or higher than that of the PDP Law. Further clarifications as to how this will be regulated will be included in the implementing regulation of the PDP Law that is yet to be promulgated.

Where a data controller wishes to send personal data to a country where the level of personal data protection is lower than the level required by the PDP Law, then the personal data controller must ensure there is adequate and binding personal data protection is available.

Where the level of personal data protection is lower than PDP Law and an adequate level of binding personal protection is unavailable, an approval through a written or recorded consent must be obtained from the data subject prior to transferring data overseas.

For clarity, data controllers only need to ensure either the adequacy level or binding personal data protection is sufficient prior to the transfer of personal data overseas.

Further, ESPs will no longer need to coordinate with the MOCI for data transfers both within and outside of Indonesia.

Additional protective measures for cross-border transfers

Currently, there are no specific obligations on organisations in Indonesia to receive approvals from local authorities or adopt or implement additional measures to protect information that is being disclosed to overseas recipients, such as binding corporate rules, standard contractual clauses. However, if necessary, organisations that conduct cross-border data transfers may ask for advocacy assistance, e.g., consultation) from the MOCI.

Once the PDP Law is in force, the data controller must ensure the existence of an adequate and binding instrument (for example, standard contractual clauses) prior to carrying out cross-border data transfer if the country to where the data is being sent does not meet the same standard of personal data protection as set out under the PDP Law.

Data sovereignty / localisation

Under GR 71/2019, ESPs operating within the public sector are required to process, manage and / or collect electronic systems and electronic data within the Indonesian jurisdiction, unless the necessary technology to store such data is not available in Indonesia. ESPs operating within the private sector are not limited as such. However, such ESPs in the private sector must be able to provide access to the electronic system and data if requested by law enforcement agencies and other relevant authorities for supervisory and law enforcement purposes. In addition, under MOCI 20/2016, ESPs that provide public services must use data and disaster recovery centres within Indonesia.

There are some industries with specific legislation (e.g., financial services) that may have an impact on where an organisation chooses or is required to maintain certain information registers or records. The application of these policies / laws would need to be considered on a case-by-case basis, having regard to the industry the organisation operates in and the types of information they collect.

COLLECTION AND PROCESSING OBLIGATIONS

As a baseline, before the PDP Law is fully in force, the relevant PDP Regulations require organisations that collect and process personal data where they have obtained express informed consent from the data owner. MOCI Reg 20/2016 goes one step further and obligates ESPs to limit the collection of personal data to only relevant and suitable information in accordance with the purpose stated at the time of collection and must be conducted accurately. The same spirit is also upheld within the PDP Law which advocates for Personal Data to be processed in accordance with its purpose and data collection to be minimized as necessary.

The PDP Law and GR 71/2019 stipulates that besides obtaining prior consent from the personal data owner, the personal data processing (including collection) must satisfy one the following requirements:

- fulfil contractual obligations in the event that the personal data owner (currently defined as data subject under the PDP Law) is one of the parties or to fulfil the request of the personal data owner upon entering into an agreement;
- fulfil legal obligations of the personal data controller in accordance with statutory provisions;
- fulfil the vital interests of the personal data owner;
- implement the personal data controller's authorities in accordance with statutory provisions;
- fulfil the obligations of the personal data controller in public services for the public interest; and/or
- fulfil the legitimate interests of the personal data controller and/or personal data owner.

In addition, a data controller is obligated to carry out a data protection impact assessment when processing personal data with a high potential risk to data subjects, which includes specific personal data.

SECURITY REQUIREMENTS

GR 71/2019 and MOCI 20/2016 require ESPs to ensure that they have taken the necessary technical and organisational measures to comply with the applicable laws and regulations, including:

- certification of electronic systems used by the ESP in accordance with the prevailing laws and regulations;
- implementing an internal personal data protection policy in processing the personal data;
- raising employee awareness to ensure the protection of personal data in the electronic system managed by the ESP; and
- organising employee training for the prevention of personal data breaches in the electronic system managed by the ESP.

Similarly, the PDP Law requires a personal data controller to protect and ensure security of personal data processed by:

- preparing and implementing operational technical measures to protect personal data from disruption in the personal data processing that is contrary to provisions of laws and regulations; and
- determining the security level of personal data by considering the nature and risks of personal data that must be protected in the personal data processing.

Personal data controllers are also required to maintain the confidentiality of personal data throughout processing activities and must protect personal data from unauthorised processing.

Data minimisation

GR 71/2019 and MOCI Reg 20/2016 provide that personal data can only be handled in accordance with the purpose for which it was initially collected (and as conveyed to the data subject).

Further, GR 71/2019 regulates the obligation for ESPs to delete personal data that is irrelevant. Personal data may be irrelevant where, for example, consent has been withdrawn, its processing is no longer in accordance with the acquisition purpose, or its utilisation has exceeded the agreed period. The obligation of deletion stipulated in the GR 71/2019 consists both of erasure and delisting from search engines.

The PDP Law also sets out certain principles of personal data protection — one such principle is that data collection should be limited and specific to the purpose.

BREACH NOTIFICATION

Currently, if there has been a failure with an electronic system or failure to protect personal data, ESPs must report this to law enforcement bodies (i.e., the Indonesian police) and the relevant sectoral ministry or agency that supervises the ESPs business activities. In addition, organisations must also provide written notice to the affected personal data owner (especially if such data breach potentially has a detrimental effect on the personal data owner) within 14 days of the ESP being aware of the breach. The notification (i) must contain the reason or cause of the failure to protect the confidentiality of the personal data and (ii) can be conducted electronically, if the personal data owner has given consent for it, at the time of obtaining and collecting its personal data.

Data breaches are referred to as "personal data protection failures" and defined as any "failure in protecting a person's personal data in terms of confidentiality, integrity, and availability of the personal data, including security breaches, whether intentional or unintentional, which lead to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed".

In the event of a personal data breach failure, the data controller must deliver written notification to **both** the data subject and the Data Protection Authority within 72 hours. The written notice shall contain, at the minimum, details regarding:

- a description of the personal data that was breached;
- when and how the personal data was breached; and
- a description of the efforts undertaken by the personal data controller to handle and mitigate the effects of the personal data breach, and any recovery action taken to date.

For serious breaches which would disrupt public services and / or significantly affect the public interest, there is also a requirement to notify the public. The PDP Law does not currently prescribe the mechanisms for public notification. However, it is expected that future implementing regulations of the PDP Law will provide further detail.

INDIVIDUAL RIGHTS AND ACTION

The PDP Law grants data subjects several rights which are listed as follows:

Right to be informed

Data subjects have the right to obtain information regarding the identity clarity, basis of legal interest, purpose of requesting and using personal data and claim accountability of parties that request personal data.

Right to access / correction

Data subjects have the right to access and obtain a copy of personal data regarding themselves in accordance with provisions of laws and regulations. They also have the right to complete, update and correct any errors and/or inaccuracies in personal data regarding themselves in accordance with the purpose of personal data processing.

Right to erasure

Data subjects shall have the right to end processing, delete and / or destroy personal data regarding themselves in accordance with provisions of laws and regulations.

Right to restrict processing

Data subjects have the right to delay or limit the personal data processing proportionally with the purpose of personal data processing.

Right to object processing

Data subjects shall have the right to object to a decision-making action that is based solely on automated processing, including profiling, which has legal consequences or has a significant impact on data subjects.

Right to data portability

Data subjects shall have the right to obtain and / or use personal data regarding themselves from a personal data controller in a form that is in accordance with the structure and/or format commonly used or readable by an electronic system.

Right to withdraw consent

Data subjects shall have the right to withdraw consent to the processing of personal data regarding themselves that has been given to a personal data controller.

Right to deletion

The data subject is entitled to end processing, delete and / or destroy personal data regarding themselves. There is also an obligation to erase the personal data once it is irrelevant (e.g., once the retention time limit of the personal data lapses).

The PDP Law distinguishes the rights of data subject into the right to delete and the right to destroy. Personal data should be deleted if:

- personal data is no longer necessary for the achievement of purposes for the personal data processing;
- the data subject has withdrawn their consent to the personal data processing;
- there is a request from the data subject to do so; or
- personal data is obtained and/or processed in an unlawful manner.

Personal data should be destroyed (i.e., personal data should be made inaccessible, non-retrievable and re-usable by any person in any way so that it can no longer be used to identify the data subject) if:

- the retention period has expired and is described as being destroyed based on the archive retention schedule;
- there is a request from the data subject to do so;
- the personal data are not related to the settlement of the legal process of a case; and/or
- personal data are obtained and / or processed in an unlawful manner.

Direct right of action

This right is known as a 'right to obtain compensation' under the PDP Law. Data subjects have the right to sue and receive compensation for violations of the processing of personal data regarding themselves in accordance with provisions of laws and regulations. However, the guidance on determining amounts or maximum amounts of the compensation is expected to be regulated under future implementing regulations of the PDP Law in the form of Government Regulation.

PRIVACY BY DESIGN AND DEFAULT

Indonesian laws and regulations do not refer specifically to the concept of "privacy by design", "privacy by default" or equivalent.

ENFORCEMENT

Currently, the MOCI has enforcement powers to issue administrative sanctions, including removal of entities from electronic system provider lists, temporary suspension of ESPs, revocation of the relevant business licences connected to any violation of the PDP Regulations, revocation of access to the relevant electronic systems and imposing administrative fines. The MOCI also has powers to block access to apps and websites that violate applicable laws and regulations. However, the MOCI's scope of authority is limited to personal data, privacy and cybersecurity in general, in which other sectoral authorities may regulate specifically depending on the sector (e.g., financial services, health, etc.).

Once the Data Protection Authority is established under the PDP Law, it will have the authority to conduct enforcement of administrative law on violations of the PDP Law. Additionally, the Data Protection Authority will assist law enforcement in handling allegations of crime in relation to personal data.

In addition, the Indonesian police have powers to investigate crimes relating to electronic transactions and data protection, such as summoning witnesses, examining individuals or organisations suspected of committing a crime, examining information technology tools suspected of being used to commit a crime and requesting expert assistance to the investigation.

Penalties / fines

Currently, non-compliance with EIT Law can result in criminal penalties ranging from an IDR 600 million to IDR 12 billion fine and up to 12 years of imprisonment, depending on the nature of the breach involved.

Failure to comply with GR 71/2019 is subject to administrative sanctions (which do not eliminate any civil and criminal liability), which could be in the form of written warnings, administrative fines, temporary suspension of ESP, termination of access to the electronic systems and expulsion from the list of registrations.

A breach of MOCI Reg 20/2016 will result in administrative sanctions in the form of verbal or written warnings, temporary suspension of ESPs and public online announcement of the breach.

The PDP Law introduces sanctions whereby non-compliance with requirements of the PDP Law that causes losses to a data subject may result in written warnings, administrative fines up to 2% of annual income or revenue for both individuals and corporations, criminal sanctions such as penal fines (up to IDR 6 billion for individuals and up to IDR 60 billion for corporations) and imprisonment up to 6 years (for individuals) or confiscation of profits obtained from criminal acts, and temporary suspension of activities and/or dissolution of the corporation.

It is important to note that criminal sanctions are enforced by the public prosecutor (and not the yet-to-be-formed Data Protection Agency), and therefore have already had effect since enactment of the PDP Law.

Consequences for breaches of data sovereignty / data localisation requirements

Breaches or non-compliance with data sovereignty or data localisation requirements may result in verbal and written warnings, temporary suspension of activities and announcement of the non-compliance by the MOCI and / or the relevant other institution that supervise the ESPs business activities (e.g., Financial Services Authority).

Directors' duties

There are no specific directors' duties that apply under the PDP Regulations. However, there are general directors' duties under Law No. 40 of 2007 on Limited Liability Companies as amended by Law No. 6 of 2023 on the Stipulation of Government Regulation No. 2 of 2022 in Lieu of Law No. 11 of 2020 on Job Creation into Law that may apply to data protection and security, including the performance of their duties in good faith, prudently and responsibly in the interests of the company and in accordance with purpose and objectives of the company. In addition, if criminal sanctions under the PDP Law are imposed on a company, such criminal sanctions can be imposed on the director as well as the management of the company according to PDP Law.

UPCOMING REFORM

Following the passing of the PDP Law, an implementing regulation in the form of a government regulation is expected to be promulgated at the latest by 2024. Amongst others, the regulation will regulate the submission of objections to automatic processing of personal data, impact assessment of personal data protection, notification procedure in case of merger, spin-off, acquisition, consolidation or dissolution of business entities and establishment of the Data Protection Authority.

JAPAN

KEY PRIVACY / DATA PROTECTION LAWS

The *Act on the Protection of Personal Information* (Act No. 57 of 2003) (**APPI**) is the main data protection law in Japan which regulates the handling of personal information by "personal information handling business operators". Personal information handling business operators are persons providing a personal information database for use in business (i.e. collecting a body of information comprising personal information). Amendments to the APPI were passed by the National Diet of Japan in 2020 and 2021. The 2020 amendments came fully into force recently on 1 April 2022. The 2021 amendments which integrate data protection laws of national government and public sectors also came into force on 1 April 2022, and the remaining amendments, which integrate data protection laws of municipal government, came into force on 1 April 2023.

All businesses that obtain and handle the personal information of Japanese residents in the course of their business must comply with the APPI. For this purpose, a "business" means activities which can be conducted repeatedly for a particular purpose and are regarded as a business under social conventions; a business can be for profit or not. Press, professional writing, religious, and political activities are excluded from the scope of the APPI.

From 1 April 2022, national government agencies and those in the public sector are also regulated through the APPI, which were regulated by the Protection of Personal Information Held by Administrative Organs and the Act on the Protection of Personal Information Held by Independent Administrative Agencies. Local governments were bound by local regulations. The remaining 2021 amendments came into force on 1 April 2023 and local governments are now also regulated through the APPI.

A number of guidelines for the handling of personal information have also been published by the Personal Information Protection Commission (**PPC**).

Personal and sensitive information

"Personal information" is defined as any information relating to a living individual and from which one can deduce the identity of a living individual. This includes biometric markers and official individual identification codes.

"Anonymously processed information" means any information about individuals from which all personal information has been removed and cannot be subsequently restored.

The recent amendments also introduced the concepts of "personally referable information" and "pseudonymously processed information". "Pseudonymously processed information" is information which has been processed from personal information in a manner that the individual can no longer be identified solely from the data. "Personally referable information" is information relating to a living individual which does not fall under the scope of personal information, pseudonymously processed information, or anonymously processed information. With reference to the PPC guidelines, personally referable information can be cookie information, a person's age, gender, or family makeup that are linked to their email address, a person's purchase history of goods and / or services, a person's location data, or a person's area of interest.

"Special care-required personal information" means personal information comprising a person's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice, or other disadvantages to the individual.

There is also certain personal information, such as Individual Numbers (the number obtained by converting a Japanese resident's record code), that are governed by other ancillary acts including *the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure* (Act No. 27 of 2013 as amended) (**My Number Act**).

REGULATOR / AUTHORITY

The Personal Information Protection Commission (**PPC**) is the central agency in Japan that acts as a supervisory governmental organisation on issues of privacy protection. It regulates both the APPI and the My Number Act. There are also other specific ministries that oversee certain industries' data.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

There is no legal obligation for organisations to appoint a DPO. However, the PPC guidelines provide that all organisations falling under the scope of the APPI must take security measures for the handling of personal information, which may include the appointment of a person in charge of the handling of personal information. There are also some sector-specific guidelines which provide data protection or similar officer requirements as industry-driven efforts to enhance data privacy.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The APPI applies extraterritorially to any business that handles personal information of Japanese residents in a foreign country in relation to its provision of goods or services provided to an individual located in Japan, regardless of where the business is headquartered.

EMPLOYEE DATA / INFORMATION

Under the APPI, employee data is regulated the same way as personal data that is collected and processed outside the employment context. There are no specific requirements for obtaining employee consents.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Unless certain conditions are met, the APPI requires prior consent to transfer personal information outside of Japan. In obtaining consent, organisations must share information about the receiving third party, including the name of the country or region where they are located, the data privacy or personal information protection systems of the third party and information relating to personal information protection measures that the receiving third party will take.

The PPC has undertaken its own research into the personal information protection systems of other countries or regions. To the extent that the third party recipient is located in a country / region covered by the PPC, then the business may provide the personal information protection system description published by the PPC in obtaining the consent of the subject person.

Consent to the transfer is not required where:

- the transferee is in a country on a white-list of countries issued by the PPC as having a data protection regime equivalent to that under the APPI (currently, the foreign countries with these standards include the UK and the countries in the European Economic Area); or
- the organisation can ensure that the recipient of the data has implemented adequate standards of data protection that are at a minimum, equivalent to the standards required under the APPI or has obtained some recognition for the use of an international data handling framework.

Organisations are required to ensure that these data protection standards are maintained and where the recipient third party is unable to maintain continuous implementation of these standards, the organisation must cease personal information transfer immediately.

In addition, the prior consent of the individual is not required if the transfer is:

- specifically required or authorised by any laws or regulations of Japan;
- necessary for protecting the life, health or property of an individual, and consent is difficult to obtain;
- necessary for improving public health and sanitation, or promoting the sound upbringing of children, and the consent of the individual is difficult to obtain;
- required by public authorities or persons commissioned by public authorities to perform their duties and obtaining the prior consent of the individual carries the risk of hindering the performance of those duties (e.g. the disclosure is required by police investigating an unlawful act); or
- required for use in academic studies that satisfies particular requirements.

Additional protective measures for cross-border transfers

Other than as mentioned above, there are no specific obligations on organisations to take any additional measures to process a cross-border transfer of personal information. In fact, transfers may take place solely on the basis of a contract or binding contractual rule if they ensure, in relation to the handling of personal information by the person who receives the provision, the implementation of measures are in line with the purpose of the provisions under APPI by an appropriate and reasonable method.

Data sovereignty / localisation

There are no data processing registration requirements, data sovereignty or data localisation requirements in Japan. However, there are some industry specific guidelines (e.g. healthcare and medical) that contain certain rules on data localisation that relevant organisations must have regard to.

COLLECTION AND PROCESSING OBLIGATIONS

Organisations may only collect and handle personal information where it has specified to the fullest extent possible the purpose of use of the information. This purpose of use must have been communicated to individuals when the personal information was collected, promptly afterwards, or by way of a public announcement, for example, on the website. Where the scope of use changes beyond the scope reasonably relevant to the prior scope, further consent from the individual must be sought.

Sensitive information may only be collected with the consent of the individual unless one of the following exceptions applies:

- required or authorised by law and regulations;
- necessary for protecting the life, health or property of an individual and consent is difficult to obtain;
- necessary for improving public health and sanitation, or promoting the sound upbringing of children, and consent is difficult to obtain;
- required by public authorities or persons commissioned by public authorities to perform their duties and obtaining the prior consent of the individual carries the risk of hindering the performance of those duties (e.g. the disclosure is required by police investigating an unlawful act);
- required for use in academic studies that satisfies particular requirements; or
- information that was made public by particular organisations.

SECURITY REQUIREMENTS

The APPI requires "necessary and proper" action to be undertaken to ensure personal information is appropriately collected, used, and stored. However, the APPI does not provide specific guidance as to what steps constitute "necessary and proper" action.

The PPC has outlined some recommended security measures through guidelines, including "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures". The PPC guidelines have also suggested that internal policies and documentation should be created in relation to security measures, a data leakage risk response framework should be developed, and organisations should execute non-disclosure contracts with employees who have access to personal information.

Data minimisation

The APPI prohibits the handling of personal information beyond "the necessary scope to achieve a utilisation purpose" i.e. inadequate data and excessively unnecessary handling of data beyond what is necessary for achieving its intended purpose is not allowed.

BREACH NOTIFICATION

Organisations are required to report data breach incidents to the PPC and affected individuals if the data breach incidents could harm the rights and interests of individuals.

Under the APPI, unless the affected data had been encrypted at a high level, the PPC and affected individuals must be notified if:

- the affected or possibly affected data contains:
  - sensitive personal information; or
  - data that would cause a financial risk in the case of unauthorised use;
- the loss is a result of intentional theft or possible theft by a third party (as opposed to just an accidental loss); or
- the number of affected or possibly affected individuals exceeds 1,000.

Notification is required "sumiyaka-ni" (promptly) (which is suggested by the PPC as within approximately three to five days, though depending on each case) upon becoming aware of the incident, and an update notification is required within 30 days (or in the case of intentional theft or possible theft, 60 days) from the time becoming aware of the incident.

Additionally, the PPC guidelines recommend that organisations investigate and take necessary preventative measures and / or publicise the nature of the breach and the steps taken to rectify the issue.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

Individuals are able to request the erasure or the cessation of use of their personal information, among others, under the following circumstances:

- if it has become unnecessary to utilise the personal information;
- if the organisation holding the personal information has been the subject of a data breach or leakage; or
- there is a possibility that handling the personal information would harm the rights or legitimate interests of the individual.

If an individual requests the erasure or the cessation of use of their personal information, the organisation must action this unless the request is unreasonable, or the cessation would be costly or would otherwise be difficult (e.g. the recall of information already distributed).

Right to access / correction

If there is a request by an individual, an organisation must disclose without delay the personal information it holds in relation to that individual. An organisation may refuse access if it would result in:

- injury to life or bodily safety, property or other rights and interest of the individual or any third party;
- a material interference with the organisation's business operations; or
- a violation of other Japanese laws prohibiting disclosure.

The recent amendments also give individuals the right to request an electronic copy of their personal information.

Individuals have the right to access an organisation's record of data transfers to third parties.

Individuals also have the right to request to revise, correct, or amend the personal data retained by an organisation when the contents of retained personal data is not correct.

Direct right of action

Individuals who have had their privacy interfered with can sue for damages in torts relating to the infringement of their privacy. Individuals may also lodge a complaint with the PPC regarding the handling of their personal information, and the PPC will conduct a mediation accordingly.

PRIVACY BY DESIGN AND DEFAULT

Whilst the APPI does not recognise the concepts of privacy by design or by default, it does, in practice, recognise that these concepts are useful to protect individual privacy rights.

ENFORCEMENT

The PPC has the primary investigatory, advisory, and enforcement powers under the APPI and the My Number Act. This regulator usually follows an enforcement pattern of an initial inquiry into allegations, followed by recommendations to correct any violations. The PPC can pursue legal action and make orders against organisations if it considers that the infringement of an individual's material rights or interests is imminent or unable to be rectified.

In limited circumstances, the PPC may allow information it has collected in investigations to be used for criminal investigations overseas.

Penalties / fines

Any organisation which fails to comply with corrective orders issued by the PPC can be liable for criminal punishment of up to one year imprisonment or fines up to 1,000,000 Japanese yen (up to 100,000,000 Japanese yen for business organisations). In addition, the recent amendments allow the PPC to publish the names of organisations who do not comply with orders.

Organisations or employees that use personal information to gain profits illegally may be subject to punishment of up to a year in prison or a fine of up to 500,000 Japanese yen (up to 100,000,000 Japanese yen for business organisations).

For completeness, we note that neither the APPI nor the Data Breach Guidelines impose any sanctions for failure to make a report or notification of a data breach.

Consequences for breaches of data sovereignty / data localisation requirements

There are no specific penalties applicable to breaches / non-compliance data sovereignty / data localisation requirements.

Directors' duties

There are no specific directors' duties that apply under the APPI. However, there are general directors' duties under the Companies Act that require directors to perform their duties in compliance with all laws and regulations and with the care of a prudent management. Neglect of their duties will result in being held liable for resulting damages.

UPCOMING REFORM

The APPI has an "every three years" (counting from the enforcement of recent amendment, 2022) review policy, with the 2020 and 2021 amendments being the most recent two amendments. The 2020 amendments to the APPI make two broad changes: giving individuals more rights over their personal information and increasing the reporting obligations of businesses. The 2021 amendments brought uniformity in data privacy and protection across both public and private sectors. The next review of the APPI is expected around 2025.

MALAYSIA

KEY PRIVACY / DATA PROTECTION LAWS

The principal privacy legislation is the Personal Data Protection Act 2010 (**PDPA**) and sets out a comprehensive data protection regulatory framework in Malaysia. The PDPA governs "personal data", which is defined as information that is:

a. in respect of commercial transactions;

b. processed or recorded electronically; and

c. relates directly or indirectly to a data subject who is identified or identifiable.

The PDPA applies to data users that process personal data in respect of commercial transactions processed within Malaysia, but does not apply to Malaysia's Federal Government and State Government.

"Data users" are defined in the PDPA as organisations that control or authorise the processing of personal data.

The PDPA is supported by the *Personal Data Protection Standards 2015* which sets out the "minimum standards" expected of data users in respect of their handling of personal data. In addition, data users must conform to the Codes of Practice issued by the Commissioner. There are currently five industry codes of practice in relation to the banking and financial sector, utilities sector (electricity), Malaysia aviation sector, Malaysia insurance and takaful sector, and communications sector. There is an additional *General Code of Practice of Personal Data Protection* (**General Code**) that was issued by the PDPC and effective as of 15 December 2022. The General Code further sets out best practices for the "data user" to meet the requirements under the PDPA. The code of practice applies to data users who are not currently subject to any other codes of practice registered under the PDPA. Sectors subjected to the General Code include, amongst other sectors:

- Retail and wholesale dealings as defined under the *Control Supplies Act 1961*
- Direct selling carried out by a licensee under the *Direct Sales and Anti-Pyramid Scheme Act 1993*
- Education
- Professional services (e.g. accounting, architecture, audit, engineering, legal, etc.)
- Tourism and hospitalities
- Real estate

The General Code is a non-exhaustive, enforceable standard for the principles in the PDPA and the rights of the data subject, including the:

- **General Principle** — outlines data user's practice in processing personal data;
- **Notice and Choice Principle** — outlines data user's responsibilities in informing data subjects when processing personal data;
- **Disclosure Principle** — outlines data user's responsibility in obtaining consent from data subject before disclosure of personal data;
- **Security Principle** — outlines the procedure for processing personal data to prevent data loss, misuse, modification, unauthorised or accidental access or disclosure, and alteration or destruction;

- **Retention Principle** — outlines requirements on the data user in relation to the retention of personal data, specifically ensuring that personal data is not kept for longer than necessary;
- **Data Integrity Principle** — outlines the responsibility of data user to ensure that personal data is kept accurate, completed and updated; and
- **Access Principle** — outlines the right of the data subject to access and correct their personal data.

REGULATOR / AUTHORITY

The Personal Data Protection Commissioner (**PDPC**) is the regulator responsible for enforcing the PDPA and the General Code.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

The PDPA does not currently include a specific requirement to appoint a DPO or privacy officer.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

As mentioned above, "personal data" essentially involves anything in respect of commercial transactions of which can be directly or indirectly related to a data subject, who is identified or identifiable from that information or from other information that data users have. However, the PDPA does not apply to federal or state government agencies or credit reporting agencies.

The PDPA also applies additional obligations to "sensitive personal data", being personal data relating to:

- physical or mental health;
- political opinions;
- religious beliefs;
- commission or alleged commission of an offence; or
- any other personal data under public order issued by the Minister of Communications and Multimedia.

Extra-territorial scope and registration

The PDPA does not generally have an extra-territorial application. The PDPA's territorial scope is limited to organisations established in Malaysia or that use equipment located in Malaysia to process personal data.

The PDPA requires data users in specified categories to register with the PDPC. The PDPC may choose to grant or refuse an application for registration, and may impose conditions upon any registration it grants.

The current categories of data users who are required to register with the PDPC (as set out in the *Personal Data Protection (Class of Data Users) Order 2013* and the *Personal Data Protection (Class of Data Users) (Amendment) Order 2016)* include communications, banking and financial institutions, insurance, health, tourism and hospitality, transportation, education, direct selling, legal, audit, accountancy, engineering or architecture, retailers or wholesalers, private employment agencies, real estate, utilities, pawnbrokers, and money lenders. The certificates of registration must be displayed at a data user's principal place of business and a failure to register is an offence.

EMPLOYEE DATA / INFORMATION

The PDPA applies to employee data in the same way as it applies to personal data collected and processed outside the employment context.

Employers must provide employees a written notice containing the following information:

- a description of the employees' personal data is being processed by or on behalf of the employer;
- the purposes for which the employee data is being or is to be collected and further processed;
- the source of that personal data;
- employees' right to request access to and to request correction of the data and the contact details for any inquiries or complaints;
- third parties to whom the employer may disclose the employee data;
- the choices and means the employer offers the employee for limiting the processing of employee data,
- whether it is obligatory or voluntary for the employees to supply the data; and
- where it is obligatory for the employee to supply the employee data, the consequences for the employee if they fail to supply the data.

Employers can collect, use and disclose non-sensitive personal information without the consent of the data subject if the processing is necessary for the performance of an employment contract.

Generally, the processing of sensitive personal data requires the explicit consent of the employee. However, as an exception, an employer may process sensitive personal data without the explicit consent of the employee if the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the employer in connection with the employment.

Cross-border data transfers of employee data are permitted where the employee has consented to the transfer (more see section "Cross-Border Transfers and Data Sovereignty" below). Consent for cross-border data transfers can be obtained through the employer's privacy notice, or in contracts between the employer and the employee, via contractual clauses which provide that the employee consents to the processing of their personal data, including the transfer of their personal data outside the country.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

The PDPA includes an express restriction on cross-border data transfers. Specifically, the PDPA requires that personal data only be transferred outside of Malaysia, if:

- the data subject has given their consent;
- the recipient is in a jurisdiction that has been specified by the relevant Minister as having "substantially similar" protections to the PDPA;
- the transfer is necessary for the performance of a contract with the data subject;
- the transfer is necessary for the performance of a contract between the data user and a third party that is either in the data subject's interests or at the data subject's request;
- the transfer is for the purpose of legal proceedings or legal advice;

- the data user has reasonable grounds for believing that the transfer is for the avoidance of adverse action against the data subject;
- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the
- personal data will be processed in the foreign country in a manner consistent with that required by the PDPA in Malaysia;
- the transfer is necessary to protect the vital interests of the data subject; or
- the transfer is in the public interest (as determined by the relevant Minister).

Additional protective measures for cross-border transfers

There is no specific requirement to put in place for additional protections (such as standard contractual clauses) for cross-border transfers of personal data. However, as described above, implementing "reasonable precautions" to ensure that personal data will be processed in a manner consistent with the PDPA is one of the lawful bases under which personal data can be transferred outside of Malaysia — contractual measures may assist meeting this requirement.

Data sovereignty / localisation

There are currently no data localisation requirements under the PDPA.

COLLECTION AND PROCESSING OBLIGATIONS

Under the PDPA, "processing" is defined to include both collecting and using personal data. The processing of personal data must only be conducted for the following legal bases:

- with the data subject's consent;
- for the performance of a contract (or other legal obligation) to which the data subject is a party, or for the taking of steps with a view to entering into a contract;
- to protect the vital interests of the data subject;
- for the administration of justice; or
- for the exercise of functions conferred by law.

In addition, any processing of personal data must be:

- for a purpose directly related to an activity of the data user;
- necessary for that purpose; and
- not excessive in relation to that purpose.

The PDPA requires data subjects to be informed of their personal data that is being processed (via a personal data protection notice), and the purposes for which it is processed. The General Code sets out further information that must be included in the notice, including third parties to whom the data will be disclosed. The General Code also provides further clarity on the manner and form in which the notice could be provided to data subjects.

In addition, data users cannot process sensitive personal data unless the data subject has given explicit consent to such processing and the processing is limited to the purposes of:

- performance of a right or obligation connected to employment;
- protecting the vital interests of the data subject or another person;
- medical purposes by a healthcare professional;
- obtaining legal advice or legal proceedings;
- administration of justice;
- for the exercise of functions conferred by written law; or
- other purposes as the Minister thinks fit.

An exception exists to the processing of sensitive personal data if the information has been made public from the steps deliberately taken by the data subject.

Consent

Where consent is required, this must be explicit consent. The *Personal Data Protection Regulations 2013* provide that consent must be recorded and properly maintained.

The General Code provides further clarity as to the manner in which consent can be collected and maintained, e.g. through a clickable box online. The General Code also specifically states that a personal data protection notice cannot be used to obtain a blanket consent from individuals.

SECURITY REQUIREMENTS

The PDPA requires data users to take "practical steps to protect the personal data" from loss, misuse, or unauthorised access. In addition, the Regulations require data users to implement a security policy which must also comply with any standards issued by the PDPC from time to time. Where processing is carried out by a processor on behalf of a data user, the data user must ensure that the data processor provides sufficient guarantees in respect of technical and organisational security measures governing the processing.

There are no specific security requirements for cross-border transfers. However, the "place or location where the personal data is stored" is one of the factors that the PDPA lists as influencing what steps will be considered "practical" to protect the personal data.

The General Code specifies that data users must maintain a 'personal data system' that can, upon request, be inspected by the PDPC. The personal data system must include, amongst other things, records of consent, the personal data protection notice provided to the individual at the time of collection, and a list of third parties to whom the data is disclosed.

The General Code also expressly requires relevant data users to develop and implement a compliance framework to ensure compliance with the General Code and the PDPA.

Data minimisation

The PDPA does not contain any explicit "data minimisation" obligations. However, personal data must not be used and collected in an "excessive" manner and should not be kept beyond what is required.

BREACH NOTIFICATION

The PDPA does not currently contain a mandatory data breach notification regime. However, the Department of Personal Data Protection encourages data users to voluntarily notify the department of a data breach involving customers personal data within 72 hours.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

The PDPA does not include a "right to erasure" or "right to be forgotten". However, personal data must not be kept longer than is necessary for the fulfilment of the purpose for which it was collected, and data subjects may withdraw their consent to data processing at any time.

Right to access / correction

The PDPA allows data subjects to request access to their personal data held by a data user and be able to correct personal data that is inaccurate, incomplete, misleading, or out of date.

Direct right of action

Individuals do not have a direct cause of action in relation to breaches of the PDPA. However, individuals may make a complaint to the PDPC of an alleged breach, in which case the PDPC may choose to investigate the complaint. In addition, individuals can consider commencing civil action in tort against a data user for any misuse of their personal data.

PRIVACY BY DESIGN AND DEFAULT

The PDPA does not include an explicit "privacy by design" requirement or requirement for privacy impact assessments to be conducted.

ENFORCEMENT

The PDPC has powers to carry out inspections of personal data systems in order to assist the Commissioner in making recommendations under the PDPA, and also investigate data users. The PDPC may also seek a warrant to search and seize materials.

Where the PDPC identifies that a data user has contravened a provision of the PDPA, it may serve an enforcement notice detailing the failure, and directing the data user to take steps specified in the enforcement notice to remedy the contravention (including ceasing to process personal data until any remediation has been completed).

Penalties / fines

The PDPA also imposes a range of fines and criminal penalties. These range from 10,000–500,000 RM fines and from 1–3 years' imprisonment. For example, failure to comply with the Personal Data Protection Standards is an offence the penalty for which is a fine of 300,000 RM or 2 years' imprisonment.

A failure to comply with the General Code may attract a fine up to 100,000 RM and/or imprisonment for up to a maximum of one year.

Directors' duties

Pursuant to the PDPA, where a body corporate commits an offence, any person who at the time was a director, CEO, COO, manager, or similar officer may also be deemed to have committed the same offence personally as the body corporate did. A defence to this offence may be available if the officer can prove that both a) the offence occurred without their knowledge or consent, and b) they took all reasonable precautions to prevent the commission of the offence.

UPCOMING REFORM

In February 2020, the Malaysian government released the Public Consultation Paper No 01/2020 on the Review of the PDPA. This consultation paper included a number of proposed reforms relating to the greater alignment of the PDPA with the GDPR, such as the introduction of data breach notification, data portability, privacy by design, extending the obligations of data processors, the appointment of a data protection officer obligations, processing personal data in the cloud, introduction of 'black-list' regime to replace the current 'white-list' regime for cross-border transfer of personal data, and extension of the application of PDPA to both federal government and state governments. A draft bill outlining these changes was tabled for the Malaysian Parliament's approval in October 2022. However, the Malaysian Parliament was dissolved in early October 2022 for the 15th general elections. The new Malaysian Government has highlighted two further areas for consideration explicitly, increased penalties for a breach of the PDPA and misuse of data and increased enforcement powers of the Department of Personal Data Protection as a potential independent statutory commission. The new Malaysian Government plans to table the proposed amendments to the PDPA for the Malaysian Parliament's approval by end of 2023.

NEW ZEALAND

KEY PRIVACY / DATA PROTECTION LAWS

Principal legislation

The principal privacy legislation is the *Privacy Act 2020* (**Privacy Act**) which includes the Information Privacy Principles (**IPPs**) that came into effect on 1 December 2020. The Privacy Act (including the IPPs) regulates the handling of "personal information" by "agencies", whether they are located in New Zealand or not.

The term "personal information" includes "information about an identifiable individual" (including information relating to a death that is maintained by the Registrar-General).

The Privacy Act applies to any person, business, and organisation (referred to in the legislation as an "agency") that holds personal information. Exemptions include courts and tribunals (where the information related to its judicial functions),news entities carrying on news activities and Members of Parliament. The Privacy Act places the onus on agencies to ensure that their collection of personal information is done in accordance with New Zealand's privacy framework.

Bill 292-1, the *Privacy Act Amendment Bill* (**Bill**) was recently introduced to Parliament. The Bill aims to impose notification obligations on agencies that indirectly collect personal information about an individual to notify that individual when they indirectly collect information about them.

Other relevant laws

There are also other laws which impose additional privacy obligations on relevant agencies, including the *Public Records Act 2005, Tax Administration Act 1994,* and the *Customs and Excise Act 2018*. If another law says something different to the IPPs, it will override the Privacy Act. In addition, some industries and types of personal information are governed by codes of practice, for example the Health Information Privacy Code and Telecommunications Information Privacy Code.

REGULATOR / AUTHORITY

The Office of the Privacy Commissioner (**OPC**) is an Independent Crown Entity. The OPC is funded by the state but is independent of government or ministerial control. The OPC has a wide variety of functions relating to the proper handling of personal information under the Privacy Act by agencies, including making public statements regarding privacy related matters, investigating privacy related complaints and breaches, helping to build privacy awareness, monitoring or enforcing compliance with the Privacy Act, and issuing codes of practice for specific industries or sectors.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

Unlike the EU GDPR, there is no requirement in New Zealand to appoint a data protection officer. However, under the Privacy Act, every agency is required to appoint at least one person as a privacy officer. Whilst the appointed privacy officer does not need to undertake any special training or hold specific qualifications, he or she should understand the IPPs.

The law does not impose any specific requirements with respect to officer location / residency and organisations may outsource / subcontract the function of a privacy officer to third parties. Privacy officers are responsible for:

- ensuring that the agency complies with the Privacy Act;
- dealing with requests from individuals looking to exercise their rights under the Privacy Act (see section titled "Individual Rights and Action" for more information); and
- working with the Privacy Commissioner during the investigation of complaints.

The Privacy Act states that anything done or omitted by the privacy officer will be treated as done or omitted by the employer or agency, whereby that act or omission results in a notifiable privacy breach (as discussed below at "Breach Notifications").

SCOPE AND EXTRA-TERRITORIAL APPLICATION

As noted above, the Privacy Act regulates the handling of an individual's "personal information" by agencies whether or not that agency is physically present in New Zealand (i.e. foreign organisations).

This means that the Privacy Act applies to any agency operating in or who "carries on business" in New Zealand, regardless of where the agency is based. Any agency that provides services to New Zealanders and / or collects their personal information for its own purposes is subject to the Privacy Act.

The extra-territorial application of the Privacy Act was considered by the Privacy Commissioner in 2018 (albeit under the Privacy Act's predecessor, the Privacy Act 1993). In its decision, the Privacy Commissioner found a large social media platform was subject to the Privacy Act and had fundamentally failed to engage with the Privacy Act. The social media platform was subject to the Privacy Act because it operated in New Zealand and provided services to New Zealanders, despite having its data processing overseas.

Definition of personal information

The term "personal information" includes "information about an identifiable individual" (including information relating to a death that is maintained by the Registrar-General).

The Privacy Act does not specifically include a definition or specific protections for "sensitive information". Although, personal information for the purposes of the Privacy Act will also include information that may be sensitive in nature provided it falls under the definition of "personal information".

The OPC has emphasised that agencies have a higher standard of care when they collect or hold sensitive information. While the Privacy Act does not specify special procedures for information that is sensitive, the obligations on organisations are stronger with respect to sensitive information and they will be held to a higher standard of accountability.

Although not defined, sensitive information can be contrasted with routine or mundane information that is about a person but is either not particularly revealing or does not reveal information that is very intimate or "private". Sensitive information is likely to include information about an individual's race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural, or political beliefs, as well as financial information.

Holding personal information for another agency

Where personal information is held by an agency (agency A) on behalf of another agency (agency B), the personal information is treated to be held by agency B. However, if agency A uses this information for their own purpose, then it will be treated as being held by agency A. Importantly, it does not matter whether agency A is in New Zealand or not, for this to apply.

EMPLOYEE DATA / INFORMATION

The Privacy Act applies to employee data in the same way as it applies to personal information collected and processed outside of the employment context. For example, the employer must follow IPP 3 — collection of information from subject. This will mean that an employer must (at the time the employee's information is collected or, if that is not practicable, as soon as practicable after the information is collected) make an employee aware of:

- the fact that information is collected;
- the purpose for which the information is collected;
- the intended recipients of the information;
- the name and address of the agency that is collecting the information;
- the name and address of the agency that will hold the information;
- whether or not the collection of the information is authorized or required by law;
- the consequences to the data subject if the requested information is not provided; and
- the rights of access to, and correction of, personal information as provided in the Privacy Act.

Generally, employees' express consent is only required for any use and disclosure of their personal information that were not notified to them at the time the information was collected (more see below "Collection and Processing Obligations" below).

For overseas transfer of employee data, employees' consent is required if they have not been previously informed of the transfer, or the foreign person/entity may not be required to protect the information in a way that provides comparable safeguards to those under the Privacy Act (more see section "Cross-Border Transfers and Data Sovereignty" below).

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

The Privacy Act restricts the transfer of personal information to overseas recipients unless certain requirements are satisfied or one of the limited exceptions apply.

In general, an organisation may disclose personal information to a foreign person or entity only if one or more of the following applies:

- if the individual concerned provides their express informed consent to the transfer after being informed by the disclosing entity that the recipient may not be subject to comparable safeguards as included in the Privacy Act;

- the recipient is carrying on business in New Zealand, and the disclosing entity believes on reasonable grounds that the recipient is subject to the Privacy Act;
- the disclosing entity believes on reasonable grounds that the recipient is subject to privacy laws that provide comparable safeguards to those in the Privacy Act;
- the disclosing entity believes on reasonable grounds that the recipient is a participant in a prescribed binding scheme;
- the disclosing entity believes on reasonable grounds that the recipient is subject to privacy laws of a prescribed country; or
- the disclosing party believes on reasonable grounds that the recipient is required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act, including pursuant to any agreement(s) entered into between the parties.

As at the date of this publication, the New Zealand Ministry of Justice has not yet prescribed any countries or binding schemes under the Privacy Act or provided any further guidance in this regard.

There are some limited exceptions under the Privacy Act to the above requirements, specifically in circumstances where the information is being disclosed for certain purposes (i.e. law enforcement, public safety, as part of court / tribunal proceedings, etc.) and it would be impractical for the above requirements to be satisfied in those circumstances.

There are no registration requirements for agencies that deal with personal information.

Additional protective measures for cross-border transfers

The use of private agreements between parties and adoption of standard contractual clauses that provide comparable protections to those found in the Privacy Act allow disclosing entities to transfer information to overseas recipients without restriction.

As noted above, the organisation must have a reasonable belief that the overseas recipient is subject to a law, or a binding scheme, comparable to the Privacy Act. It is the responsibility of the organisation to be able to justify its reasonable belief. From a practical perspective, this may involve obtaining independent legal advice as evidence of the steps taken to form their view or belief.

Data sovereignty / localisation

Outside of the above cross-border transfer restrictions, there are no specific data sovereignty or localisation requirements (such as governmental consent, approval, or registration requirements) under the Privacy Act.

When planning the disclosure of personal information outside of New Zealand, agencies may however, need to have regard to any applicable obligations under Te Tiriti o Waitangi and have an understanding of Te Ao Māori when handling personal and collective information, particularly where the agency has statutory obligations (e.g. from Treaty settlements) to engage with iwi. Māori Data Sovereignty recognises that Māori data should be subject to Māori governance. These may have a data sovereignty or data localisation effect.

COLLECTION AND PROCESSING OBLIGATIONS

Agencies may only collect personal information for a lawful purpose connected with a function or an activity of the organisation and the collection is reasonably necessary for that purpose. The collection must only occur for a lawful purpose and directly from the individual, unless an exception applies (i.e. the individual's consent is obtained or required for law enforcement purposes, public safety, as part of court / tribunal proceedings, etc.). The Privacy Act does not define the term "lawful purpose" and does not provide specific examples of what constitutes a lawful purpose. However, the OPC's guidance notes that it is important for agencies to understand their purposes for collection because this needs to be articulated to individuals.

In some situations, agencies may utilise unique identifiers in their operations but only where an identifier is necessary to enable the agency to carry out their functions efficiently. There are limitations on the use of unique identifiers:

- An agency may assign a unique identifier (i.e. it cannot be the same identifier as assigned to the individual by another agency) to an individual for use in its operations only if that identifier is necessary to enable that agency to carry out one or more of its functions efficiently.
- The agency must take reasonable steps to ensure that a unique identifier is assigned only to an individual whose identity is clearly established and the risk of misuse of a unique identifier by any person is minimised (e.g. by showing truncated account numbers on receipts or in correspondence).
- An agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.

Consent

The Privacy Act does not require agencies to obtain the express consent of an individual before collecting their personal information as long as the agency satisfies the requirements set out in IPP 3 (that is, the agency has been open about the need for the collection of personal information and intended uses) and makes the individual aware of the circumstances of collection. The agency must not use the personal information other than for the purpose for which it was obtained and the personal information must not be disclosed for any reason but for that which it was obtained, unless an exemption applies.

SECURITY REQUIREMENTS

Agencies must ensure the protection of personal information it holds by putting in place such security safeguards as are reasonable in the circumstances. This means that an organisation that holds personal information must take reasonable steps to protect the information from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure.

Data minimisation

Agencies must only collect personal information that has a lawful purpose connected with one or more of its functions or activities, effectively embedding a requirement to minimise the collection and storage of information. The agencies' "lawful purpose" may be qualified under the Privacy Act or other legislation, for example, the *Employment Relations Act 2000, Health (Retention of Health Information) Regulations 1996, Public Records Act 2005,* and *Tax Administration Act 1994*.

In addition, agencies must not keep personal information for longer than is required for the purposes for which the information may lawfully be used. This means that agencies must take steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the Privacy Act (i.e. the agency no longer has a lawful purpose to retain the information).

BREACH NOTIFICATION

There are mandatory data breach reporting requirements under the Privacy Act. A privacy breach occurs when an organisation who holds personal information either intentionally or accidentally:

- provides unauthorised or accidental access to personal information;
- discloses, alters, loses, or destroys personal information; or
- prevents someone from accessing their personal information on a temporary or permanent basis (e.g. where it is encrypted by ransomware).

Where a "notifiable data breach" occurs, the organisation must notify the OPC and the individuals affected. A "notifiable data breach" occurs when an organisation has reasonably judged that a breach it has experienced either has caused or is likely to cause serious harm (e.g. physical harm, financial fraud, family violence, psychological harm).

When assessing the likelihood of serious harm occurring as a result of the breach, the organisation should have regard to any mitigating factors including (but not limited to) any action taken by the organisation to reduce the risk of harm following the breach, whether sensitive information was involved, the nature of the harm that may be caused to affected individuals, and whether the information is protected by a security measure.

If the data breach is notifiable, agencies must inform the OPC as soon as practicable after becoming aware that a notifiable privacy breach has occurred and, unless an exception applies, the affected individuals. The OPC's expectation is that notification will occur within 72 hours. Not all privacy breaches will need to be reported and the OPC has a helpful online tool called NotifyUs to assist agencies determine whether a breach is notifiable or not.

Agencies that fail to notify the OPC of a notifiable privacy breach can be liable to a fine of up to NZD 10,000. The OPC may also issue compliance notices, which also carries a fine of up to NZD 10,000 for non-compliance.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

There is no specific "right to erasure" under the Privacy Act. However, agencies must take reasonable steps to destroy or de-identify the information if it is no longer needed for any purpose permitted under the Privacy Act.

Rights to access / correction

Upon request, organisations must give an individual access to their information and take reasonable steps to correct personal information to ensure that it is accurate, up-to-date, complete, relevant, and not misleading.

Direct right of action

If an individual believes their information has not been handled in accordance with the Privacy Act, they are expected to consult with the organisation in question (through that organisation's privacy officer) first to resolve the issue. If this does not get resolved or if they are unsatisfied with the response, the individual may request that the OPC investigates. This is discussed further in the "Enforcement" section below.

A general tort of invasion of privacy exists in New Zealand and there have been several judgements handed down by New Zealand courts recognising this right to privacy.

PRIVACY BY DESIGN AND DEFAULT

Although there is no specific requirement for agencies to adopt "privacy by design", the OPC recognises the importance of agencies adopting a "privacy by design" approach when developing products and services.

Agencies are encouraged to manage privacy risks proactively rather than take a reactive approach to addressing any privacy risks that are identified. This requires an understanding of the potential "privacy impacts" of a particular project before the project commences / is deployed.

Agencies are encouraged to undertake privacy impact assessment (**PIAs**). In its simplest form, a PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating those impacts to ensure the agency is meeting their legal obligations.

ENFORCEMENT

The OPC may seek fines for the criminal offences of misleading an organisation in order to access, use, alter or destroy someone else's information, destroying documents containing personal information if a request has been made for it, or failing to notify the OPC of a notifiable privacy breach. The penalty for these offences is a fine up to NZD 10,000. The OPC has powers to issue compliance notices requiring agencies to take certain actions or cease certain activity in order to comply with the Privacy Act. Any failure to follow OPC notices leaves the individual liable to a fine up to NZD 10,000.

In relation to individual privacy complaints, the OPC's role is to determine if there has been an interference with privacy and to facilitate a resolution between the parties. If the OPC is unable to resolve a dispute relating to a breach, the matter may be referred to the Human Rights Tribunal (**HRT**). While it operates in an informal way, the HRT has the same powers as a district court and can make binding decisions, award damages (up to a maximum of NZD 350,000) and order parties to pay costs.

Consequences for breaches of data sovereignty / data localisation requirements

Although there are no specific penalties applicable to breaches of or non-compliance with data sovereignty / data localisation requirements, if a breach of an agency's obligations with respect to cross-border transfers is investigated by the OPC and then later referred to the HRT, penalties of up to NZD 350,000 could be imposed (depending on the seriousness of the breach). In addition, every person who fails to comply with a transfer prohibition notice on the transfer of personal information outside New Zealand is liable on conviction of a fine of up to NZD 10,000.

Directors' duties

There are no specific directors' duties imposed under the Privacy Act. However, there are general directors' duties under the New Zealand *Companies Act 1993* that may apply to data protection and security, including the duty to exercise due care, diligence and skill that a reasonable director would exercise in the same circumstances.

UPCOMING REFORM

The Government has released a draft of the Customer and Product Data Bill for consultation. This draft Bill proposes the introduction of new "consumer data rights" to consumers and small businesses in order to access and share their data with trusted third parties. The banking sector will be the first industry participating. Following this consultation period, the Government is expected to introduce the Bill to Parliament towards the end of 2023.

The Government has also introduced the Bill (as outlined in the "Key Privacy / Data Protection Laws" section above), which requires individuals to be notified when personal information is collected indirectly, from a third party source. This is aimed at giving individuals a more complete picture as to who has their information, and brings New Zealand in line with Australia, the EU and UK. The public will be given an opportunity to provide submissions in relation to the Bill in 2024.

THE PHILIPPINES

KEY PRIVACY / DATA PROTECTION LAWS

The *Data Privacy Act of 2012* **(DPA)** is the governing law on data privacy matters in the Philippines. It is supported by the *Implementing Rules and Regulations of the DPA* (**IRR**).

In addition, there are certain sectoral laws that include provisions which regulate the handling of personal information. For example, the Cloud First Policy of the Department of Information and Communication Technology which includes obligations on data processed by government entities, and the Bangko Sentral ng Pilipinas (**BSP**) which regulates data processed by banks and other BSP-supervised financial institutions (**BSFIs**).

REGULATOR / AUTHORITY

The National Privacy Commission (**NPC**) is an independent body established in early 2016 with the primary objective to administer and implement the DPA and to ensure the Philippines' compliance with international standards set for data protection.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

Under the DPA and its IRR, personal information controllers (**PIC**) and personal information processors (**PIP**), being any natural or juridical person or other body involved in the processing of personal data) are required to appoint a compliance officer for privacy or a DPO, who will be accountable for ensuring compliance with the appropriate data protection laws and regulations. The law does not impose any specific requirements with respect to DPO location / residency and organisations may outsource / subcontract the function of a DPO to third parties (for more information, please refer to NPC Advisory No. 2017–01, on Designation of Data Protection Officers).

Data Processing Systems Registration

In December 2022, the NPC issued *Circular No. 2022–04* (**Circular**) which sets out the registration framework of DPOs and data processing systems (**DPS**). Under the Circular, PICs and PIPs that meet any of the criteria for registration, are required to register their respective DPO and DPS to demonstrate its compliance with the DPA, IRR and other relevant issuances of the NPC.

PICs and PIPs operating in Philippines are required to register with the NPC if they meet any of the following criteria:

- the PIC has more than 250 employees;
- the PIC processes sensitive personal information of at least 1000 individuals; or
- those processing information will pose a risk to the rights of the data subjects.

PICs and PIPs covered by the scope of the Circular, but that do not meet any of the above criteria, are not required to register with the NPC, but are required to submit a sworn declaration attesting to the fact that they are not covered by the registration requirement.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The DPA broadly applies to any natural or juridical persons involved in the processing of personal information, including any operation or any set of operations performed upon personal information.

The law has extra-territorial application and therefore also applies to foreign organisations who process information about a Philippine citizen / resident, use equipment located in the Philippines for processing, or maintain an office, branch, or agency in the Philippines.

There are different types of personal information regulated under the PDA: personal information, sensitive personal information, and privileged information.

"Personal information" refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. In essence, it captures any information that can make an individual readily identifiable.

"Sensitive personal information" refers to personal information about:

- an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations;
- an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- information issued by government agencies peculiar to an individual (including, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns); and
- any information specifically established by an executive order or an act of Congress to be kept classified.

"Privileged information" refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication (for example, information shared by a client to their lawyer).

EMPLOYEE DATA / INFORMATION

The DPA and the IRR apply to all types of personal information, including employee data.

Employers can process personal information if one of the legal bases applies (for more details, see section "Collection and Processing Obligations" below.) For non-sensitive personal information, consent is not required if the processing is necessary for compliance with legal requirements or performing an employment contract.

However, the processing of sensitive personal information is generally prohibited with some exceptions (for more details, see section "Collection and Processing Obligations" below). One of the exceptions is where employees have given their specific consent, specific to the purpose prior to the processing. In this case, employers must provide comprehensive information about how they handle sensitive personal information, enabling employees to freely and knowingly consent to that processing.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

The DPA does not prohibit the transfer of personal information to foreign jurisdictions if consistent with the general data processing requirements stipulated under the DPA. Where personal information is further processed by a third party (known as, data sharing) in the private sector, consent must be obtained accordingly. It does not recognise or consider the data protection regulations of other countries. However, it should be noted that the organisation controlling the data remains accountable for any personal information under its control or custody that have been transferred to third party processors, whether domestically or internationally.

There are certain sectoral regulations on cross-border data transfer of government and financial information. The Cloud First Policy of the Department of Information and Communication Technology establishes storage, security, and encryption requirements for government-held information. Financial information relating to inherent or core banking functions cannot be transferred offshore. There are also some additional audit and confidentiality requirements.

Additional protective measures for cross-border transfers

There are no specific requirements to take any additional protective measures to process a cross-border transfer. However, there are general provisions that prescribe that data sharing "for commercial purposes, including direct marketing, shall be covered by a data sharing agreement". The data sharing agreement must establish adequate safeguards for data privacy and security, and uphold the rights of data subjects.

The law does not explicitly prescribe binding corporate rules as necessary to process a cross-border transfer but in practice, certification has helped an organisation discharge its responsibility for exporting "personal information originally under its custody or its control".

Data sovereignty / localisation

Organisations operating in the Philippines involved in the collection and processing of personal information must register their data processing systems with the NPC where:

- it employs at least 250 employees;
- the processing includes sensitive personal information belonging to at least 1,000 individuals;
- the processing is not occasional; or
- the processing is likely to pose a risk to the rights and freedoms of data subjects.

Certain organisations are mandated to register their data processing systems regardless of the above criteria, including banks, government bodies, telecommunication networks, business processing outsourcing companies, insurance providers, pharmaceutical companies engaged in research, hospitals, schools, and training institutions.

Apart from the above registration requirement, there are no specific data localisation requirements in the Philippines governing personal information.

COLLECTION AND PROCESSING OBLIGATIONS

Personal information must only be collected for a specified and legitimate purpose. This purpose must be expressly declared to the individual holding the personal information before, or as soon as reasonably practicable after collection. Organisations must ensure that the information is fit for purpose, i.e. is adequate, accurate and kept up to date (where necessary).

There are also specific legal bases for the processing of personal information, which is dependent on the type of personal information involved.

Personal information

The processing of personal information may be permitted if:

- the individual has given consent;
- it is necessary and is related to the fulfilment of a contract with the individual, or in order to take steps at the request of the individual prior to entering into a contract;
- it is necessary for compliance with a legal obligation to which the data controlling organisation is subject to;
- it is necessary to protect vitally important interests of the individual, including life and health;
- responding to national emergency, complying with the requirements of public order and safety, or fulfilling functions of public authority which necessarily includes the processing of personal data for the fulfilment of its mandate; and
- it is for the purposes of the legitimate interests pursued by the data controlling organisation or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the individual which require protection under the Constitution of the Republic of the Philippines.

Sensitive and privileged information

Broadly, the processing of sensitive data and privileged information is prohibited in the Philippines. The exceptions to the blanket rule are as follows:

- the individual has given consent specific to the purpose for processing (in the case of privileged information, all parties to the exchange have given their consent prior to processing);
- the processing is necessary to protect the life and health of the individual or another person, and the individual is not legally or physically able to express consent prior to the processing;
- existing laws and regulations allow for the processing of that information (provided that the laws guarantee protection of the information and consent of the individuals is not required by such law or regulation);
- the processing is necessary to achieve the lawful and non-commercial objectives of public organisations and their associations, and the processing is confined to the bona fide members of the organisations and the data is not on-transferred to third parties, and consent was obtained;
- the processing is necessary for purposes of medical treatment and an adequate level of protection of personal data is ensured; or
- the processing is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defence of legal claims, or when provided to government or public authority.

For completeness, we note that there are certain types of information that are excluded under the material scope of the DPA, including information that falls within matters of public concern, personal information necessary for banks, other financial institutions and other public authorities, personal information processed for research, journalistic, artistic, or literary purpose, in order to uphold freedom of speech, of expression, or of the press.

SECURITY REQUIREMENTS

Data controlling organisations must act in accordance with the guidelines issued by the NPC and actively implement organisational, physical, and technical measures to protect personal information against any type of accidental, or unlawful destruction. Some appropriate safeguards include developing security policies on personal information processing, implementing corrective mitigating actions against security incidents, regularly monitoring security breaches and prevention processes.

The organisation is obligated to ensure that third parties processing personal information on its behalf shall implement the security measures required by the DPA.

Data minimisation

Personal information shall only be collected for relevant use, that is, for the fulfilment of the declared, specified, and legitimate purpose or for the purposes of legal claims.

BREACH NOTIFICATION

A "personal data breach" occurs when there is an accidental or unlawful loss, destruction, modification, unauthorised disclosure, or access to personal data. Organisations have a notification requirement where a "personal data breach" event occurs when:

- the personal data involves sensitive personal information or any other information that may be used to enable identity fraud;
- there is reason to believe that the information may have been acquired by an unauthorised person; and
- the organisation or the NPC believes that the unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Organisations are required to notify the NPC and the affected individuals within 72 hours from the knowledge of, or when there is reasonable belief that, a personal data breach requiring notification has occurred. The notification should be submitted to the NPC through written or electronic form and detail the nature of the breach, the personal information likely to have been involved, and measures taken by the entity to address the breach.

Notification is not required if the NPC determines that the notification would not be in public interest or in the interests of the affected individuals, or that the notification is unwarranted given the compliance activity undertaken by the organisation.

In addition, the NPC levies a general requirement on data controlling organisations and processors to produce an annual report summarising all security incidents and personal data breaches from the previous calendar year.

The DPA stipulates both criminal and administrative consequences for organisations who intentionally or by omission conceal / fail to notify the NPC of an occurrence of a security breach. Specifically, offenders may face imprisonment ranging from one year and 6 months to 5 years and a fine of not less than PHP 500,000 but not more than PHP 1,000,000.

INDIVIDUAL RIGHTS AND ACTION

Right to be informed

Individuals whose data is in question have the right to receive information on whether their personal data has been, currently being, or has previously been processed. Organisations must provide individuals with clear privacy notices containing information such as a description of the personal data, the purposes of processing, the recipients, the identity of the PICs or PIPs that will be given access to personal data.

Right to data portability

Individuals have the right to obtain their personal information from the PIC and / or have the same transmitted from one data controller to another, if the processing is based on consent or contract.

Right to erasure / blocking

Individuals have the right to suspend, withdraw or order the blocking, removal, erasure or destruction of their personal information if they have withdrawn consent or they have a reasonable basis to believe that the data is incomplete, outdated, false, or unlawfully being obtained or used, or the data concerns information that violates or is prejudicial to the individual.

Right to access / rectification

Individuals have a right to obtain a copy of any personal information relating to them held by an organisation (i.e. data portability). It should be provided in an easy-to-access format, accompanied with a full explanation executed in plain language.

Individuals also have the right to dispute and have corrected any inaccuracy or error in any personal information held. The organisation should act on it immediately and accordingly, unless the request is vexatious or unreasonable. Once corrected, the organisation should ensure that the data subject receives a copy of both the new and retracted information. Upon request, the organisation must also provide such information to relevant third parties.

Right to file a complaint

Individuals who are the subject of a privacy violation or personal information breach can file their complaints for violations of the DPA to the relevant PIC / PIP in the first instance. If the PIC or PIP does not address the concern adequately, individuals can then file a complaint directly with the NPC. They can pursue individual personal actions, representative action (brought by a consumer or data privacy body) and class actions through the judicial process, where courts will decide appropriate penalties and compensation.

Right to damages

An individual has the right to damages or indemnification for any damages sustained as a result of personal data being inaccurate, incomplete, outdated, false, unlawfully obtained, or used without authorisation. This includes seeking damages for any infringements on their rights and freedom as data subjects.

PRIVACY BY DESIGN AND DEFAULT

The DPA itself does not refer specifically to the concept of "privacy by design and default" but it is based on the GDPR, which adopts those concepts in its law, and it is understood that these principles be adopted by organisations. Further, the NPC, in its Advisory Note for the designation of DPO roles and responsibilities, has explicitly mentioned the impact and importance of "privacy by design".

ENFORCEMENT

The NPC is responsible for ensuring organisations comply with the obligations under the DPA. It has the power to receive, investigate, facilitate, or enable settlement of complaints. The NPC can also adjudicate and award indemnity on matters affecting any personal information. It often prepares and publicises reports on disposition of complaints and resolution of any investigation it initiates.

Additionally, the NPC can issue cease and desist orders, and impose a temporary or permanent ban on the processing of personal information upon finding that the processing will be detrimental to national security and public interest. However, it does not have criminal prosecution powers.

Penalties / fines

A breach of privacy and data protections under the DPA will give rise to administrative, civil, and criminal liabilities.

The penalties provided in the DPA and its IRR range from six months to seven years of imprisonment, together with fines ranging from PHP 100,000 to PHP 5 million based on whether personal information or sensitive personal information is involved. Moreover, additional penalties may apply depending on the identity of the offender and the number of affected individuals.

Consequences for breaches of data sovereignty / data localisation requirements

There are no "data sovereignty or data localisation" requirements, and therefore no specific penalties applicable to this.

Directors' duties

If the offender is a corporation, partnership, or any other juridical person, the penalty levied on them shall be imposed upon the responsible officers (namely, the DPO, or where there is no DPO appointed, the head of the organisation who participated in, or by their gross negligence, allowed the improper disposal of personal information or processed personal information for unauthorised purposes). If the offender is a foreign individual, he or she may be deported without further proceedings after serving the penalties prescribed.

In addition, the NPC 2022-04 Guidelines on Administrative Fines impose administrative penalties on any PIC or PIP violating the DPA, the IRR and any NPC issuances. The maximum fines can amount to up to 3% of the annual gross income of the immediately preceding year but not more than 5,000,000 million pesos (approx. USD 88,900).

UPCOMING REFORM

There is one major bill that has been pending before the Philippine Senate since August 2021 that seeks to amend the DPA, being *HB09651: An Act Strengthening the Regulatory Framework On Data Privacy Protection, Aligning With International Standards, Challenges, And Other Cross-Border Data Processing Concerns, Amending For The Purpose Republic Act No. 10173, Otherwise Known As The "Data Privacy Act Of 2012"*. The proposed amendments broadly include:

- modifying the definition of terms by adding the biometric data, genetic data, personal data, personal data breach.
- expanding the definition of data subject, personal information controller, and processing;
- expanding the sensitive personal information to include biometric and genetic data, labour affiliation, sexual orientation and identification numbers;
- narrowing exemptions from the DPA to specific sections related to lawful basis of processing. In particular, the requirements related to the lawful processing of personal information and sensitive personal information will not apply to processing of certain categories of information for the purpose of allowing public access to information that fall within matters of public concerns, information relating to a benefit of a financial nature conferred on an individual upon discretion of the government, processing of information for research purposes, processing of information collected from residents of foreign jurisdiction being processed in the Philippines, processing information that is necessary to carry out the function of public authorities, processing of information by courts actin in their judicial capacity, processing of information by the COA to carry out their audit function, and processing of information of a natural person for household activity;
- clarifying the extraterritorial application of the DPA by specifying clear instances when the processing of personal information of Philippine citizens and / or residents is concerned, if the processing is found or established in the Philippines, being done in the Philippines;
- extending the function of the NPC issue summons, subpoena and subpoena duces tecum, imposing administrative sanctions, providing assistance for the effective implementation of the act, conduct seminars and training, publishing disposition reports of complaints;
- modifying the functions and organisational structure of the NPC by adding the extra function to the NPC including powers to issue summons and subpoena, to hold and punish those violating the act, impose administrative fines, provide assistance to the implementation of the DPA, conduct of seminars or trainings, prepare reports on dispositions and resolutions and to protect the data subjects while ensuring the effectivity of the act.
- modifying the General Data Privacy Principles, explicitly stating the requirement to implement appropriate security safeguards for processing;
- modifying the criteria for lawful processing of personal information for data subjects of more than and below 15 years of age;

- modifying the exception to processing sensitive personal information and privileged information, adding extra stipulations when a data subject provides their consent; when it is necessary for the performance of the contract; when it is for the interest of public safety, when processing is with appropriate safeguards of foundations, association or any other non-profit organization for its legitimate activities; when the processing if for medical, social care and services purposes; when it is processed for the interest of public health or emergency; and when the processing is necessary solely for the archiving purposes in the public interest.
- modifying the right of the data subject, right to be informed by adding stipulations for automated decision making, adding the intentions for further processing information, sources of personal information collected, to where it will be transferred, contact details of the DPO, criteria for retention period;
- amending the section by adding the rights to reasonable access, right to object, right to rectification, right to erasure, and right to claim damage;
- including limitations on rights of data subject if it's for the public interest or when provided by law or regulation to protect life and of data subject;
- modifying security of personal information whereas if there is an unauthorized access, NPC should be notified within a 72-hour period upon being aware;
- modifying principle of accountability adding the designation of a Data Protection Officer;
- modifying applicability to Government Contractor by mandating strict procedures in a formal contract to be followed by independent contractors, consultants, or service providers engaged by government agency;
- renaming the section from Accessing Personal Information and Sensitive Personal Information Due to Negligence to Providing Access to Personal Information and Sensitive Personal Information Due to Negligence and adding stipulations;
- adding stipulation on improper disposal of personal and sensitive information, processing of personal and sensitive information for unauthorized purposes, unauthorized access or intentional breach, malicious disclosure, and unauthorized disclosure;
- renaming the Concealment of Security Breaches Involving Sensitive Personal Information to Concealment of Personal Data Breaches Involving Sensitive Personal Information and adding stipulations to the penalties;
- amending the penalty for the combination of acts with the consideration of either imprisonment or fine or both;
- expanding the conditions for the offense committed by the Public Officer; and
- modifying the restitution including the administrative sanctions, additional stipulations and paragraphs to describe further the responsibility of the NPC in terms of sanctions, administrative, awarding civil indemnity.

However, given the rigorous process of passing a law in the Philippines, it is unlikely that this bill will be passed into law within the next 12 months.

SINGAPORE

KEY PRIVACY / DATA PROTECTION LAWS

The principal privacy legislation in Singapore that governs the collection and use of personal data by organisations is the *Personal Data Protection Act of 2012 of Singapore* (**PDPA**). There are also various regulations governing the handling of personal data, including but not limited to the *Personal Data Protection (Notification of Data Breaches) Regulations 2021,* the *Personal Data Protection Regulations 2021 and the Personal Data Protection (Do Not Call Registry) Regulations 2013*.

These laws and regulations are complemented by advisory guidelines issued by the Personal Data Protection Commission (**PDPC**). These guidelines are advisory in nature and are not legally binding. However, the guidelines provide insight into how the PDPC may interpret the PDPA.

The data protection instruments mentioned above do not apply to public agencies. The public sector obligations with respect to privacy are contained in the *Government Instruction Manual on Infocomm Technology and Smart Systems Management* and *the Public Sector (Governance) Act 2018*, which mirror many of the PDPA obligations applicable to the private sector.

There are also various industry-specific laws and codes which may regulate the handling of personal data. For example, the *Banking Act 1970* governs the protection of personal data held by banks, whilst the *Code of Practice for Competition in the Provision of Telecommunication Services 2012* governs the handling of personal data by telecommunications providers.

REGULATOR / AUTHORITY

The PDPC was established in January 2013 to administer and enforce the PDPA and is the key regulatory authority for matters relating to personal data in Singapore and represents the Singapore Government internationally on data protection related issues.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

It is a requirement for organisations to appoint at least one individual to oversee data protection responsibilities and ensure the organisation's compliance with the PDPA. The business contact information of the DPO(s) should be made available to the public either through the BizFile+ website or made easily accessible on the company's website. The contact details, including the telephone number, should be Singaporean.

There is no requirement for a DPO to be located in Singapore. However, the DPO should be readily contactable from Singapore or otherwise available during normal Singapore business hours.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The PDPA governs the collection, use and disclosure of personal data by organisations.

The current definition of "personal data" has been drafted in a way to be technologically neutral such that it captures personal information in many forms (including electronic files) and "personal data" is defined to be mean "data, whether true or not, about an individual who can be identified from that data; or who can be identified from that data and other information to which the organisation has or is likely to have access".

This broad definition encompasses information such as sensitive information, health information, credit information, employee record information and tax information about an individual.

The PDPA does not define "sensitive information". However, guidelines published by the PDPC suggest that personal data of a sensitive nature such as financial information, together with other identifying information may expose an individual to the risk of fraud and identity theft, and such personal data of a sensitive nature should be subjected to a higher standard of protection. Additionally, organisations are generally not allowed to collect, use or disclose personal identification numbers (e.g. NRIC, foreign identification numbers, work permit numbers, passport numbers, birth certificate numbers) unless an exception applies (e.g. where it is required by law, necessary for the purposes of personal identity verification to a high degree of accuracy). Additionally, this information should only be retained by organisations if required by law.

The PDPA defines the term "organisation" to mean any individual, company, association or body of persons, corporate or unincorporated whether or not formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore. Accordingly, the PDPA applies extraterritorially to the extent that an organisation uses, collects, or discloses personal data in Singapore regardless of the location of the organisation's physical presence and regardless of whether or not some processing of personal data takes place outside of Singapore.

Generally, the main PDPA obligations are not imposed on:

- any individual acting on a personal or domestic basis;
- any individual acting in their capacity as an employee with an organisation; and
- any public agency in relation to the collection, use or disclosure of personal data.

EMPLOYEE DATA / INFORMATION

The PDPA applies to employee data in the same way as it applies to personal data collected and processed in other contexts. There are no specific requirements for obtaining employee consents. However, organisations may collect, use and disclose personal data without consent in certain circumstances, including but not limited to, where this is necessary for evaluative purposes. The term "evaluative purpose" is defined in section 2(1) of the PDPA and includes, amongst other things, the purpose of determining the suitability, eligibility or qualifications of an individual for employment, promotion in employment or continuance in employment.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

In relation to transfer of personal data outside of Singapore, the PDPA requires that organisations take appropriate steps to ascertain whether, and to ensure, that the receiving organisation is bound by legally enforceable obligations to provide a standard of protection to the transferred personal data that is at least comparable to the protection under the PDPA. The "legally enforceable obligations" to be imposed on the recipient of the data include obligations:

- under law;
- under any contract which must specify the countries and territories to which the personal data may be transferred under the contract;
- under binding corporate rules (which must set out the recipients of the personal data, the countries to which personal data may be transferred under the binding corporate rules, and the rights and obligations provided by the binding corporate rules); or
- under other legally binding instruments.

However, an organisation will be taken to have satisfied the requirement if the individual whose personal data is being transferred consents to the transfer — subject to certain prescribed conditions.

An organisation may apply to the PDPC to be exempted from the requirement prescribed under the PDPA. Any exemption will be subject to conditions as the PDPC determines from time to time.

Data sovereignty / localisation

There are no data processing registration requirements in Singapore. In addition, there are no specific data localisation, residency, or sovereignty requirements. However, as noted above, there are certain requirements that must be met before personal data can be disclosed to overseas recipients including by obtaining consent.

COLLECTION AND PROCESSING OBLIGATIONS

Legal basis for processing

The PDPA does not include the concept of having a "legal basis" for processing personal data.

Instead, the PDPA has outlined scenarios under which an organisation may use, collect, or disclose personal data:

i. where it is required by law;

ii. where an organisation has obtained express consent from the individual prior to the collection, use, or disclosure of the personal data (and such consent must not be a condition of providing a product or service, beyond what is reasonable to provide such product or service; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices);

iii. where there is deemed consent from the individual for the collection, use or disclosure of the personal data (e.g. where a contract has been entered into with the individual); or

iv. where the limited specific exclusions in the PDPA apply (e.g. matters affecting legitimate public interests, business asset transactions).

Express consent is obtained by informing the individual of the purpose of the use, collection and processing of the personal data and having been informed of such, the individual consents for the purpose provided.

The specific exclusions for the consent requirement include, but are not limited to, the following:

- vital interests of individuals including where it is necessary to respond to an emergency that threatens the life, health or safety of an individual or another individual, or for contacting the next of kin or a friend of any injured, ill or deceased individual;
- where it is in the national interest;
- where it is solely for artistic, literary purposes, archival or historical purposes;
- where it is collected by a news organisation solely for its news activity;
- where it is in the legitimate interests of the organisation or another person and the interests outweigh the adverse effects on the individual;
- where it is in the context of a business asset transaction;
- where it is between related organisations for business improvement purposes; and
- where the data has already been disclosed by a public agency.

Do Not Call (DNC) provisions

The Do Not Call (**DNC**) provisions of the PDPA generally prohibit organisations from sending marketing messages or causing the messages to be sent to Singapore phone numbers listed in the relevant DNC Registry. Specifically, the PDPA requires an organisation to:

- obtain valid confirmation that the phone number is not listed on the DNC Registry before sending the messages (including calls or text messages), unless the recipient has given clear and unambiguous consent to the sending of the specified message to that number;
- include in the specified message information identifying the sender of the messages and details on how the sender can be readily contacted and such details should be reasonably likely to be valid for at least 30 days after the sending of the message; and
- for voice calls, not conceal or withhold the calling line identity from the recipient.

An exception exists for sending messages to individuals with whom the organisation has an ongoing relationship, and the sole purpose of which relates to the subject matter of the ongoing relationship. Further exceptions are set out in the Eighth Schedule to the PDPA.

Prohibitions relating to the use of dictionary attacks and address-harvesting software

The PDPA prohibits the sending of messages with a Singapore link to phone numbers generated or obtained through the use of dictionary attacks and address-harvesting software. An "address-harvesting software" is one that is specifically designed or marketed for use for searching the internet for phone numbers and collecting, compiling, capturing or otherwise harvesting those numbers. A "dictionary attack" is defined as a method by which the phone number of a recipient is obtained using an automated means that generates possible phone numbers by combining numbers into numerous permutations.

SECURITY REQUIREMENTS

The PDPA places a general obligation on organisations to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or loss of personal data.

Organisations are required to ensure that personal data is not retained for any longer than is necessary, such as when the original purpose for collecting the personal data is no longer being served by the retention of the information or when retention is no longer necessary for legal or business purposes.

The *Personal Data Protection Commission's Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Guidelines on PDPA Key Concepts)* also provides guidance on what is reasonable and appropriate in the circumstances in order to fulfil the security requirements, including:

- the nature of the personal data;
- the form in which the organisation collects personal data, such as physically or electronically; and
- the possible impact to the individual concerned if an unauthorised person obtained, modified, or disposed of the personal data.

Data minimisation

Under the PDPA, an organisation must limit its collection, use, or disclosure of personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

In addition, organisations are required to ensure that personal data is not retained for any longer than is necessary, such as when the original purpose for collecting the personal data is no longer being served by the retention of the information or when retention is no longer necessary for legal or business purposes.

BREACH NOTIFICATION

A data breach occurs where there is unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data or the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification, or disposal of the personal data is likely to occur. A data breach is a notifiable data breach if the data breach:

a. results in, or is likely to result in, significant harm to an affected individual; or

b. is, or is likely to be, of a significant scale (at least 500 individuals affected).

A data breach is deemed to result in significant harm to an individual if the data breach relates to, inter alia, an individual's full name, alias or identification number, an individual's account name or number or any password, security code or data that is used or required to allow access to or use of an individual's account.

Where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach. This should generally be done within 30 calendar days, and the organisation must document all steps taken in assessing the data

breach. Where a data breach is notifiable, an organisation must notify the PDPC as soon as practicable but in any case, no later than 3 calendar days after an organisation concludes that the data breach is notifiable.

In general, the organisation must also notify each individual affected by a notifiable data breach in a manner that is reasonable in the circumstances. Effective notification to affected individuals provides them with the opportunity to take steps to protect their personal data following a data breach, such as changing their account passwords or being alert to possible scams resulting from the breach. This is, however, subject to various exceptions, *inter alia*, such as where the organisation takes any remedial action that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

The notification to the PDPC and affected individuals must include the information prescribed in the *Personal Data Protection (Notification of Data Breaches) Regulations 2021*.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

There is no specific "right to be forgotten" under the PDPA. However, as noted above, organisations are required to ensure that personal data is not retained for any longer than is necessary, such as when the original purpose for collecting the personal data is no longer being served by the retention or where retention is no longer necessary for legal or business purposes.

Right to access / correction

Individuals have a right of access to their personal data including details regarding how their personal data may have been used or disclosed in the year prior to the request. This is subject to a range of exemptions such as where the access may disclose the personal data of another individual.

Furthermore, an individual may request that an organisation correct any error or omission in an individual's personal data that is in the possession or under the control of the organisation. Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation must correct the personal data as soon as practicable, and send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation (or to selected organisations that the individual has consented to), within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose. Where the organisation is unable to fulfill the request within 30 days upon receiving the request, it must inform the individual of the time in which the request will be fulfilled.

Direct right of action

Individuals have a right of private action if they are impacted by a contravention of the PDPA. In such private actions, the court may grant relief by way of injunction or declaration, damages, any other relief as the court thinks fit.

PRIVACY BY DESIGN AND DEFAULT

The PDPA requires that organisations develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA. Furthermore, the PDPC has issued guidance such as the *Guide to Data Protection Practices for ICT (info-comm technology) Systems* which provides a compilation of data protection practices from past PDPC advisories and guides, and recommends basic and enhanced practices that organisations can incorporate into their ICT systems.

ENFORCEMENT

Penalties may be imposed for breaches of the PDPA. The amendments to the PDPA (which came into effect on 1 October 2022) increased the maximum financial penalty which may be imposed on organisations for any intentional or negligent contravention of the data protection provisions to up to SGD 1 million or 10% of the organisation's annual turnover in Singapore (for organisations with annual local turnover exceeding SGD 10 million).

For any intentional or negligent contravention of the DNC prohibition involving the use of dictionary attacks and address-harvesting software, individuals may be required to pay a financial penalty of up to SGD 200,000 and in the case of an organisation, a financial penalty of up to SGD 1 million or 5% of the organisation's annual turnover in Singapore (where the organisation's annual turnover in Singapore exceeds $20 million). For contraventions of other DNC provisions, the PDPC may require payment of a financial penalty of up to SGD 200,000 in the case of an individual and in any other case, a financial penalty of up to SGD 1 million.

When determining financial penalty, an organisation's annual turnover in Singapore will be ascertained from the most recent audited accounts of the organisation available at the time the financial penalty is imposed.

Officers, partners, or persons involved in management may also be held criminally liable for an organisation's violations in certain circumstances. Furthermore, individuals may commence a private action in which case the court may grant relief by way of injunction or declaration, compensation, damages, or any other relief as the court thinks fit.

Under the PDPA, the PDPC has the power to refer matters to alternative dispute resolution, carry out investigations, accept voluntary undertakings, make directions, review an organisation's refusal to provide access to personal data or make a correction requested, register a direction or written notice in the district court for enforcement, and/or impose a financial penalty.

UPCOMING REFORM

The *Personal Data Protection (Amendment) Act 2020* contains a new Part VIB relating to data portability whereby. organisations must, at the request of an individual, transmit an individual's applicable personal data, in an electronic form, that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. Whilst there has been no specific timeframe given for the right to data portability to come into effect, the PDPC has indicated that it will be working closely with all stakeholders for a phased implementation of Part VIB, and that its implementation can be expected once new regulations are issued.

SOUTH KOREA

KEY PRIVACY / DATA PROTECTION LAWS

The central law relating to data protection and privacy in South Korea is the *Personal Information Protection Act 2011* (as amended in 2020) (**PIPA**) and its supporting regulations.

In addition to the PIPA, there are sectoral laws that regulate the handling of personal information. Most prominently, the *Use and Protection of Credit Information Act* (**UPCIA**) protects credit information in the banking and finance sector. Additionally, the *Act on Promotion of Information and Communications Network Utilization and Information Protection* (**ICNA**, Information and Communications Network Act) protects the personal information of those who use information and communication network services, although the PIPA remains the primary legislation that governs the personal information protection obligations of the Information and Communication Service Providers (**ICSPs**).

REGULATOR / AUTHORITY

The Personal Information Protection Commission (**PIPC**) is an independent body established under PIPA to regulate and protect the privacy rights of individuals. The key role of the PIPC is to deliberate on and resolve personal information-related issues, and coordinate different opinions among other government agencies on the processing of personal information.

The Financial Services Commission (**FSC**) serves as the competent authority in relation to the UPCIA.

The Korea Communications Commission (**KCC**) serves as the competent authority in relation to the ICNA.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

A chief privacy officer (**CPO**) (who must be a representative or executive) must be appointed to any organisation that is a personal information controller (that is, any person, government entity, company, or other person that, directly or through a third party, controls and / or processes personal information in order to operate personal information files as part of its activities). The law does not impose any specific requirements with respect to CPO location / residency.

In the event that a CPO is not appointed, the personal information processing organisation may be subject to an administrative fine of up to KRW 10 million.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The PIPA is applicable to all organisations that handle data and any outsourced data processors within South Korea. Its extra-territorial application is not explicitly referenced or defined within the law, however in practice, the approach is understood to be similar to the GDPR. In addition, there have been a number of foreign companies that have been fined or warned by the PIPC over privacy violations. Accordingly, foreign organisations that target South Korean users (regardless of whether the organisation provides services targeted at Koreans or generates revenue from doing business in South Korea) are likely to be caught within the ambit of enforcement action under PIPA.

Data regulated by the PIPA includes both personal and sensitive information. “Personal information” means information pertaining to any living person that makes it possible to identify such individuals by their name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information and pseudonymised information, being information incapable of identifying a particular individual without the use of additional information).

“Sensitive information” is personal information concerning an individual’s ideology, belief, labour union membership, political views or membership in a political party, health or sex life, genetic information, criminal history, physical, physiological, or behavioural characteristics, racial or ethnic information, and other personal information that can markedly threaten the privacy of an individual.

EMPLOYEE DATA / INFORMATION

The PIPA governs notice and consent requirements with respect to employee information. The provisions of PIPA that generally apply to personal information also apply to employee information. Accordingly, the collection, processing and transfer of employee information must comply with PIPA, but the Department of Labor and Employment has also issued some guidance specific to employee information:

- The minimum information necessary for hiring and employment contract purposes (such as place of residence, expertise, work experience and performance results, which are necessary for job assignment, evaluation and granting of benefits) may be collected and processed without consent.
- A prospective employee must be notified of the scope of the information collected for these purposes.
- Sensitive information and unique identification data (residential registration number, passport number, driver's license number, and alien registration number) may not be collected or processed without the employee's consent.
- An employee's consent is not required to transfer employee information, such as salary information, to the appropriate government agencies for social security withholding purposes, as long as the transfer is made in accordance with applicable social security laws. However, information related to an employee's job transfer or promotion may not be transferred without the employee's consent.
- If employee information is transferred to a third party as a result of a corporate reorganization (e.g., sale of business, merger, etc.), the employee must be notified prior to the transfer and has the right to opt out of the transfer.
- Collecting information about an employee's biometrics is generally prohibited. If such information must be collected, it must be done on an exceptional basis and with the employee's consent.
- Upon termination of employment, the employee's personal information must be destroyed immediately, but the minimum information necessary to provide proof of employment must be retained for at least three years and must be kept and maintained separately from the data of current employees.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

An organisation may not transfer personal information to a foreign third party without obtaining the consent of the individual. Prior to receiving consent, the organisation must advise the individual of certain information, including the following:

- the specific information to be transferred overseas;
- the destination country;
- the date, time, and method of transmission;
- the name of the third party and the contact information of the person in charge of the personal information within the third party;
- the third party's purpose of use of the personal information and the period of retention and usage; and
- the individual's right to refusal and the consequences of such refusal.

Exceptions to the consent requirement exist where the personal information is transferred to an overseas third party for the purpose of processing or storing the personal information in order to enter into and enforce the contract with the individuals. So long as the above information is notified to individuals according to the data controller's personal information processing policy or in writing (including e-mail), no consent from the individual is required.

In addition, individual consent is not required in any of the following circumstances:

- where the law, a treaty to which Korea is a party, and other international agreements provide for the protection of personal information transferred abroad;
- where the transferee of personal information is certified by the PIPC and has taken measures to protect the personal information transferred and to implement certified matters in the country of the transferee; or
- where the information is transferred to a country where the PIPC determines that the protections afforded in that country are equivalent to the protections afforded under the PIPA.

Apart from the exceptions set out above, the consent requirements may not be waived under any circumstances when the personal information is transferred to an overseas third party.

Additional protective measures for cross-border transfers

There are specific obligations on organisations to take additional protective measures for cross-border transfers, including organizing the internal control system in place and encrypting the information to be transferred.

Data sovereignty / localisation

Under the PIPA, there is no general rule regarding the registration of organisations that handle personal information. However, a public institution which manages a personal information file (i.e. collection of personal information) must register certain information with the PIPC, including the name of the information file, the basis and purpose of the operation of the file, the categories of personal information recorded on the information file, the method to process the file, and the period of information retention.

Apart from the above requirements, there are no specific data sovereignty or localisation requirements (such as governmental consent or approval requirements) under the PIPA. However, there are some sector-specific requirements that will need to be considered as it may have an impact on where an organisation chooses or is required to maintain certain information registers or records. For example, the *Regulation on Supervision of Electronic Financial Transactions* prescribes that finance companies headquartered in Korea must have their data centre and disaster-recovery centre located in Korea.

COLLECTION AND PROCESSING OBLIGATIONS

The PIPA requires personal information to be collected for specific and lawful purposes and not be used for further incompatible purposes.

An organisation may initially collect and use personal information:

i. with the consent of an individual;

ii. where there are special provisions in an Act or it is inevitable to fulfil an obligation imposed by or under an Act or subordinate statute;

iii. where it is inevitable for a public institution to perform its affairs provided for in an Act or subordinate statute;

iv. where it is necessary for entering into and performing a contract with an individual;

v. where it is necessary for physical safety and property interests of an individual or a third person; or

vi. where it is necessary for the personal information controller's legitimate interests, and this interest takes precedence over the rights of an individual (though this condition is limited to cases where the information is substantially relevant to a personal information controller's legitimate interests and reasonable scope is not exceeded); and

vii. where there is an urgent need to protect public health and safety.

Further processing of personal information may be allowed if it does not infringe the interests of an individual or a third person, and if the processing is reasonably related to the original purpose for which the information was collected.

The PIPA applies additional conditions where the processing is by a public institution.

There is a general prohibition on the processing of sensitive personal information. However, sensitive information may be processed if a law requires or permits it, or if separate consent has been obtained from the individual.

An organisation may process pseudonymised information without an individual's consent for the purposes of statistics, scientific research, and record keeping in the public interest. In these circumstances, when the information is transferred to a third party, no information that may be used to identify a particular individual should be included. If the identifying information is created in the course of pseudonymizing information, the data controller must stop the pseudonymization and take back and destroy the information. The data controller must also specifically address the pseudonymization process in its privacy policy.

SECURITY REQUIREMENTS

In processing any personal information or sensitive personal information, organisations must implement the following technical, administrative, and physical measures in accordance with the guidelines prescribed by the Presidential Decree in order to prevent the loss, theft, leakage, alteration, or destruction of personal information:

- establish and implement an internal control plan for handling personal information in a safe way;
- install and operate an access control device, such as a system for blocking intrusion to cut off illegal access to personal information;
- measures for preventing fabrication and alteration of access or log records;
- measures for security, including encryption technology and other methods for safe storage and transmission of personal information; and
- measures for preventing intrusion of computer viruses, including installation and operation of vaccine software, and other protective measures necessary for securing the safety of personal information.

Data minimisation

Organisations must only collect the minimum amount of personal information necessary and cannot refuse to provide goods or services where additional personal information is not supplied.

BREACH NOTIFICATION

Where organisations become aware that personal information has been inappropriately divulged (that is, a data breach has occurred), organisations must notify the individuals without delay of the details and circumstances, and the remedial steps planned. "Data breach" or "breach" is not specifically defined under the PIPA. However, the PIPC has provided guidance that to the effect that a data breach is taken to have occurred when an organisation loses control over personal information or allows access to personal information by an unauthorised person in one of the following situations:

- loss or theft of a document, portable storage drive, laptop where personal information is stored;
- access to a database where personal information is stored by an unauthorised person;
- data controller intentionally or negligently hands over a document or a storage device where personal information is stored to an unauthorised person; or
- other instances where personal information is handed over to an unauthorised person.

The Korean courts interpret "data breach" in accordance with the above standards, and in some notable cases, have further indicated that so long as the data is placed outside of the data controller's control such that an unauthorised person may access the data, a data breach will have occurred even if the unauthorised person did not actually obtain the data.

Where the number of affected individuals is 1,000 or more, organisations are required to immediately notify individuals and report the result of measures taken to the PIPC or the Korea Internet & Security Agency (**KISA**).

Additionally, there are special provisions that apply to ICSPs in relation to a data breach. ICSPs are obligated to provide individual notices to online service users and file a personal information leakage report with the details of the leakage and the remedial steps planned to the PIPC or KISA. There are

no exceptions linked to the number of affected individuals. Where an ICSP discovers an incidence of intrusion, it must report it to the Ministry of Science and ICT (**MSIT**) or KISA within 24 hours of knowledge of the intrusion, and analyse causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

If an organisation fails to adopt necessary measures for data security pursuant to the PIPA which results in a data breach, it may be subject to both administrative sanctions and criminal penalties. The PIPC may impose and collect a penalty surcharge not exceeding KRW 20 million or up to 2 years' imprisonment. Corrective orders may also be issued e.g. termination of any activities that infringes on personal information or the temporary suspension of personal information processing. Any loss, theft, divulgence, or damage specific to resident registration numbers can result in a monetary fine of up to KRW 500 million.

Further, ICSPs that fail to take the necessary measures to ensure data security of personal information can be fined up to 3% of its revenue relating to the violation.

INDIVIDUAL RIGHTS AND ACTION

Right to erasure

An individual who has reviewed their personal information held by the personal information controller may request that their personal information be corrected or deleted. However, there are certain instances which limit such rights, such as when retention of personal information is required by law.

Under the PIPA, an individual has the right to request suspension of the processing of their personal information. Unless there are grounds for refusing such a request, the organisation must suspend the partial or entire processing of the individual's personal information without delay.

Right to access / correction

An individual has the right to request access to their personal information that is being processed.

An individual who accesses their personal information has the right to request rectification or deletion of their personal information. Upon receiving such a request, information must be rectified or deleted immediately (unless an exception applies).

Direct right of action

An individual suffering from psychological or economic loss from a breach of the PIPA may commence a civil action by filing a claim for compensation from the organisation. Where individuals believe their rights have been infringed upon, they can also file a complaint to the PIPC. The PIPC may conduct an investigation and, in doing so, request relevant materials, such as articles and documents, from the organisation.

If the PIPC deems that there is substantial ground for infringement with respect to personal information, and failure to take action is likely to cause damage that is difficult to remedy, it may order the infringing organisation to take corrective measures to prevent further infringement, temporarily suspend personal information processing or recommend disciplinary action against the individual (including the representative and the executive officer in charge) responsible for violation of the PIPA and / or other data protection-related statutes.

Right to data portability

An individual may request the data controller to transfer his or her data to himself or herself or to a government-designated entity as authorised by that individual. The information that may be transferred in response to such a request is limited to information that can be processed by information processing equipment, such as a computer. Information generated by analysis and processing by the data controller is excluded from the information that can be transferred in response to the exercise of the individual's right to data portability.

The right to be excluded from automated decision-making

An individual may object to automated decision making (including decision making using artificial intelligence technology) if such decision making materially infringes the individual's rights or materially affects the individual's obligations.

PRIVACY BY DESIGN AND DEFAULT

The data protection and privacy laws in South Korea do not specify any requirements that will trigger the application of a "privacy by design" or "by default" concept. However, the PIPA and its respective implementing regulations set forth detailed standards on the technical and managerial measures to be taken with respect to personal information processing systems and network security.

ENFORCEMENT

Where a breach of personal information handling occurs, the PIPC may take an incremental approach and instruct, advise, and make recommendations to the organisation handling personal information. Where recommendations are not taken, the PIPC has the power to issue a corrective order.

The PIPC handles complaints or remedial procedures relating to personal information processing and mediation of disputes over personal information. In doing so, it can impose administrative fines, penalty surcharges, corrective orders, and other administrative sanctions.

The PIPC also can exchange and cooperate with international organisations and foreign personal information protection agencies to protect personal information.

Penalties / fines

There are a number of enforcement measures for breaches of the PIPA.

The sanctions for a particular breach of the PIPA will depend on the type and seriousness of the violation and include criminal fines, surcharges, penalties, and imprisonment. Where personal information has been transferred to a third party without the consent of the individual, both the transferor and the transferee (if it received the personal information knowing that the individual had not given consent) can be subject to criminal sanctions (imprisonment of up to 5 years or a criminal fine of up to KRW 50 million).

For all data controllers, including ICSPs, a fine can be calculated as 3% of the company's total revenue minus the amount of revenue that the data controller can prove is unrelated to the violation. The burden is on the data controller to prove how much of its revenue is unrelated to the violation. Organisations

may also face a penalty surcharge of up to 3% of their entire revenue for processing pseudonymised information in order to identify a particular individual.

The PIPC can also issue corrective orders, such as an injunction, suspension, or other protective measures. A breach of a corrective order issued by the PIPC in relation to any breach of an obligation not to provide personal information to a third party will lead to an administrative fine of up to KRW 30 million.

Consequences for breaches of data sovereignty / data localisation requirements

There are no specific penalties applicable to breaches of or non-compliance with "data sovereignty or data localisation" requirements.

Directors' duties

There are no specific directors duties that apply under the PIPA. However there have been instances where Korean courts have held an organisation and its CPO liable for the organisation's failure to have appropriate technical and administrative measures that resulted in a security breach.

UPCOMING REFORM

Draft implementing legislation for the PIPA relating to the right to opt out of automated decision making, qualification requirements for a data protection officer, and the right to data portability were expected to be announced in October 2023, but have yet to be released.

TAIWAN

KEY PRIVACY / DATA PROTECTION LAWS

The central law relating to data protection and privacy in Taiwan is the Taiwan Personal Data Protection Act (**PDPA**) and the Enforcement Rules of the Personal Data Protection Act (**Enforcement Rules**). The PDPA applies to both the private and public sectors, including individuals in Taiwan (together referred to here as "agencies").

There are also other regulations and rulings issued by various competent authorities for industry sectors that govern Taiwanese privacy and data protection, including the Insurance Act, the Financial Holding Company Act, and the National Sports Act. If an offence against computer security is involved, then the criminal sanction of the Criminal Code of the Republic of China may apply.

REGULATOR / AUTHORITY

The National Development Council (**NDC**) maintains overall responsibility for interpreting the PDPA. However, the enforcement is to be carried out by either the authorities that regulate and supervise the business operations of agencies in various industries e.g. the Financial Supervisory Commission (**FSC**) is in charge of regulating personal data protection matters involving financial institutions, or the municipality / city government that has jurisdiction over the business operations in question.

A recent amendment to the PDPA introduced a new and exclusive competent regulatory authority for personal data protection, known as the Personal Data Protection Commission (PDPC). Whilst this amendment came into effect on 2 June 2023, the preparatory office of the PDPC is estimated to be established in October 2023, and the new PDPC is expected to be established in 2024.

DATA PRIVACY OFFICER (DPO) REQUIREMENT

There is no requirement to appoint a DPO under the PDPA.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The PDPA applies in principle to all data collection and processing activities taking place in Taiwan without regard to whether the data subjects are Taiwanese nationals or not. It materially covers the scope of all personal and sensitive data.

The PDPA defines "personal data" as a natural person's name, date of birth, identity card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, details of his or her sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning his or her social activities and any other information that may be used to directly or indirectly identify that person.

Personal data pertaining to an individual's medical records, healthcare, genetics, sex life, physical examination and criminal records is categorised as "sensitive personal data" and is subject to special protection.

Currently, the PDPA does not explicitly provide for the extra-territorial application of the PDPA to offshore entities.

EMPLOYEE DATA / INFORMATION

The PDPA applies to employee data in the same way as it applies to personal data collected and processed outside the employment context. Employers must therefore comply with the same PDPA obligations when collecting, processing and using employee data.

Where employers collect personal information from employees, it must inform them of the following information at the time of collection:

- the purpose(s) for which the data is being collected;
- the types of personal data to be collected;
- for how long, where, by whom and in what manner the data will be used;
- the rights that the employee may exercise in relation to their personal data under Article 3 of the PDPA and how they can exercise them; and
- how the employees' rights or interests will be affected if he or she chooses not to provide the data.

Employers may then process employee data within the specific purpose for which it was collected, unless an exception applies (see section "Collection and Processing Obligations" below). As part of the processing, employers may also transfer employee data to foreign territories, unless the government otherwise issues an order or ruling that prohibits such a transfer (see section "Cross-border Transfer and Data Sovereignty" below).

Employers may collect and use sensitive personal information such as medical records only in limited circumstances, for example, where the employers have obtained valid written consent, or it is specifically stipulated by law (see section "Collection and Processing Obligations" below).

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Personal data may be transferred outside of Taiwan (as long as it is still based on one of the legal bases as set forth under the PDPA — see *"Collection and processing obligations"* below). Accordingly, there is no strict requirement for additional consent in relation to cross-border transfers. Personal data may be freely transferred to foreign territories, unless the government otherwise issues an order or ruling that prohibits or restricts such a transfer on one of the following reasons:

- where any material national interest is involved;
- the transfer is prohibited or restricted under an international treaty or agreement;
- the country to which the personal data is to be transferred does not provide sound legal protection of

- personal data, thereby it may be affecting / jeopardising the rights and interests of the data subjects; or
- the purpose of the transfer to a third country (territory) is to evade restrictions under the PDPA.

In practice, there are few government rulings restricting the international transfer of personal data. In 2012, the National Communications Commission has issued a ruling which prohibits telecommunications operators from transferring subscribers' personal data to China. More recently, the Ministry of Health and Welfare also issued a ruling which prohibits social worker offices from transferring clients' personal data to China.

Additional protective measures for cross-border transfers

Provided the transfer is pursuant to a legal ground set out below, there are no specific obligations on organisations to take any additional practical measures for the purposes of cross-border transfer.

Data sovereignty / localisation

There are no specific data sovereignty or localisation requirements (such as governmental consent, approval, or registration requirements) under the PDPA. In addition, Taiwan does not have a registration requirement for data processing activities within its region.

However, the competent authority of each industry sector may issue specific regulations relating to the issue of data localisation. For example, pursuant to the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation issued by FSC, if the processing of customer data is outsourced to cloud service providers by financial institutions, the location for storage of the personal data shall be within the territory of Taiwan unless 1) the financial institutions reserve their rights to designate the location of data processing, and 2) the data protection requirements at the location of storage are more stringent than those of Taiwan. Regardless, backup copies of important client information need to be kept within Taiwan unless otherwise approved by the competent authority.

COLLECTION AND PROCESSING OBLIGATIONS

Any agency collecting personal data must provide data subjects with a privacy notice and expressly inform data subjects of certain information, including the name of the collection agency, the purpose of the collection, the categories of the personal data to be collected, the time period, territory, recipients, and methods of which the personal data is used, the data subject's rights and the methods for exercising such rights, and how their rights and interests will be affected if they elect not to provide their personal data.

The obligation to provide a privacy notice may be waived in certain circumstances, including where it is prescribed by law, where notice will harm public interests or where the data subject is already aware of the contents of the notification.

Further, a non-government agency must have a specific purpose for collecting, processing, or using personal data and it must occur on one of the following bases:

- it is specifically permitted by law;
- where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data;

- the data is already in the public domain due to disclosure by the data subject or in a legitimate manner;
- the processing is necessary for an academic research institution to gather statistics or conduct academic research in the public interest, provided that any information sufficient to identify the data subject has been removed;
- the consent of the data subject has been obtained;
- it is necessary to enhance the public interest;
- the data has been obtained from a source that is accessible from publicly available sources, unless the interests of the data subject surpass; or
- the processing will not harm the data subject's rights or benefits.

Personal data must only be used within the scope of the specific purpose for which it was collected unless its additional use is allowable under the PDPA. Allowable uses such as where further consent has been obtained, the use is necessary to promote a public interest, necessary to prevent a risk to the life, body, freedom, or property of the data subject, necessary to prevent material harm to the rights or benefits of third parties, necessary for academic research in the public interest or the use will benefit the data subject.

There are limited circumstances where sensitive personal data may be collected, processed, or used.

These circumstances include where:

- it is specifically stipulated by law;
- the information is necessary for a government agency to perform its legal duties or for a non-government agency to fulfil its legal obligations, and proper security measures are adopted prior or subsequent to such collection, processing or use;
- the data subject has made such information public or the information has been publicised legally;
- the information is necessary to collate statistics or conduct other academic research by a government
- agency or an academic research institution for the purpose of medical treatment, public health or crime prevention, as long as the information does not lead to the identification of a specific person after its processing by the provider or its disclosure by the collector;
- the information is necessary to assist a government agency in performing its legal duties or a non-government agency in fulfilling its legal obligations, and proper security measures are adopted prior or subsequent to such collection, processing or use; or
- the data subject has freely consented in writing and the use of such information does not exceed the necessary scope of the specific purpose, and no other restrictions under any other statute apply.

Consent

Where agencies expressly inform data subjects when first collecting their personal data, and the privacy notice meets the requirements as prescribed under the PDPA and agreed by the data subject, then it will be considered that the consent has been given by the data subject. Consent may be presumed if the data subject does not expressly object to the privacy notice and has already provided his or her personal data.

This presumption of consent, however, does not apply in the case of sensitive personal data since only "written consent" will suffice the requirement for collection, processing and use of sensitive personal data.

Where data is used beyond the scope of the specific purpose for which it was collected, additional legal reason (e.g. consent) will also be required.

SECURITY REQUIREMENTS

The PDPA requires that agencies that control data to adopt appropriate security and maintenance measures to safeguard the personal data that it holds. Any third party processors of data should also take appropriate security measures in compliance with the requirements set out by the competent authority(ies) of the controller(s). Where it fails to do so, the agency controlling the data will be held liable for such non-compliance.

The Enforcement Rules define "proper security and maintenance measures" to be technical or organisational measures taken by agencies for the purpose of preventing personal data from being stolen, altered, damaged, destroyed or disclosed. It further sets out recommended measures to safeguard personal data, such as allocating management personnel and reasonable resources, establishing a mechanism for risk assessment and management of personal data, establishing a mechanism for preventing, giving notice of and responding to data breaches, promoting awareness, education and training, establishing an audit mechanism for data security and implementing integrated and persistent improvements to the security and maintenance of personal data.

In addition, certain industry sectors (e.g. hospitals, financial institutions, recruitment agencies) may have guidelines issued by the relevant competent authority which requires security measures for personal data files.

Data minimisation

There are no explicit data minimisation requirements set out in the PDPA. However, the concept of data minimisation is embedded in the PDPA, which requires that the collection, processing, and use of personal data should only be made for the necessary scope of the purpose for which it was collected.

BREACH NOTIFICATION

Under the PDPA, there is no general requirement to report an incident to authorities where personal data is stolen, disclosed, altered, or otherwise infringed as a result of a violation of the PDPA. However, the affected data subjects must be notified in a proper manner after the agency controlling the data has investigated the incident. The notification must include details of the infringement of personal data and the measures which have been taken in response.

Further, the Enforcement Rules provides that the notification must be made in a timely manner. If individual notification would be too costly, notification may be made online, through the news media or through another appropriate disclosure manner, after taking technical feasibility and data subject's privacy protection into account.

Notwithstanding the above, the regulation governing financial institutions was amended late in 2021 requiring non-government agencies to report to the competent authority within 72 hours of an occurrence of a material personal data breach.

INDIVIDUAL RIGHTS AND ACTION

Data subjects enjoy certain rights under the PDPA that they may exercise in relation to their personal data. These rights cannot be waived in advance or limited contractually.

Right to erasure

Data subjects have the right to request erasure of their personal data. Where the collection, processing or use of the personal data is in violation of the PDPA or the specific purpose for which the data was collected no longer exists or the term has expired, agencies must erase the personal data.

Right to access / correction

Data subjects have the right to access their personal data to review and request a copy of it. They also have the right to correct or supplement their personal data. Agencies must cease the processing or use of personal data if there is any dispute over the accuracy of the personal data, unless one of the following situations has been met and the dispute has been recorded:

- the processing or use is necessary for the performance of a government agency's statutory duties or a non-government agency's business operation; or
- the data subject has given written consent.

Direct right of action

Data subjects can seek private remedies from the agencies for a breach or interference of privacy in Taiwan. They may also raise a complaint with the relevant competent authorities for any breach of the PDPA. A data subject may seek compensation if an agency has intentionally or negligently breached the PDPA and such breach results in an infringement on their right to privacy. If it is difficult to prove the actual damage, data subjects may request the court to consider the severity of infringement and determine the amount of compensation between NTD 500 to NTD 20,000 for each violation. Where a class action is brought, the total compensation available to a class is up to NTD 200,000,000.

PRIVACY BY DESIGN AND DEFAULT

There are no specific requirements for privacy by design or default under the PDPA. However, the Enforcement Rules suggest that organisations should establish a mechanism to evaluate the risk of collecting, processing, and using personal information. There are also sector-specific laws and regulations or guidance on establishing cybersecurity systems that apply the concepts of "privacy by design" or "privacy by default". For example, the Life Insurance Association of the Republic of China and the Non-Life Insurance Association of the Republic of China provide prescriptive self-regulatory rules which contain concepts of privacy by design / default in relation to handling cybersecurity and data protection.

ENFORCEMENT

While the NDC is the main authority for interpretations of the PDPA, the actual enforcement powers rest with each relevant sectoral competent authority as well as the municipal governments. These authorities can carry out audits and inspections and can impose fines on agencies that are in breach of the PDPA. The authorities also have advisory and corrective powers.

On 2 March 2023, the Executive Yuan passed the "Refined Measures to Prevent Personal Data Leakage of Non-government Agencies" which instructed the various authorities to set up administrative inspection teams to strengthen corrective capabilities for high-risk businesses, and for recent high-profile personal data leakage cases of social concern.[1]

Penalties / fines

As mentioned above, an agency intentionally or negligently breaches the PDPA and such breach results in interference or violation with a data subject's right to privacy, it will be liable to compensate the data subject for the damages suffered. The maximum amount of damages where the data subject cannot provide evidence for the actual damage amount is NTD 20,000 per violation.

However, these limits may be circumvented by commencing action in general causes of action in tort over and above the specific statutory cause of action created by the PDPA, provided that actual damages can be proved.

Violations of the PDPA can also result in administrative sanctions (the regulator has the power to impose an administrative fine of between NTD 20,000 and NTD 500,000 repeatedly until the required action is taken) and criminal sanctions (up to five years' imprisonment and / or fines of up to NTD 1,000,000) where the agency violated the PDPA with the intention to gain "benefit" for themself or a third party or to "harm" the interests of others and thereby cause damage to others.

Based on the latest amendment of PDPA which came into force on 2 June 2023, the cap of the administrative fines increased to NTD 2,000,000 in the situation that non-government agency violates its security maintenance duties. If an agency fails to rectify the violation within a specified period, it will subject to NTD 150,000 to NTD 15,000,000 administrative fines consecutively per violation. In a serious violation situation, the administrative fines increased to NTD 150,000 to NTD 15,000,000 in the first place. And for those failure to rectify, the fines will be imposed consecutively per violation.

Consequences for breaches of data sovereignty / data localisation requirements

Where a breach had malicious intent and violated a specific order or decision relating to the restrictions on cross-border transfers made by the sectoral competent authority, the violator is subject to both administrative (fines between NTD 50,000 and NTD 500,000) and criminal sanctions (up to five years' imprisonment and / or fines of up to NTD 1,000,000).

Directors' duties

There are no specific directors' duties that apply under the PDPA, but any natural or legal person who intentionally or negligently breaches the PDPA is liable for damages arising from illegal collection, processing or use of personal data.

[1] National Development Council, https://www.ndc.gov.tw/nc_27_36901.

UPCOMING REFORM

In 2019, the NDC solicited public comments and opinions on proposed amendments to the PDPA, including adopting the same restrictions on international transfers of personal data as applied under the GDPR, requiring agencies to notify the government authority of a data breach, combining the three legal concepts of "collection", "processing" and "use" of data under the PDPA into one — "processing", etc. It is likely that in the near future the NDC will propose draft amendments to align the PDPA with the GDPR and to obtain an adequacy decision from the European Commission.

THAILAND

KEY PRIVACY / DATA PROTECTION LAWS

The main data protection law in Thailand is the Personal Data Protection Act B.E. 2562 (2019) (**PDPA**), which became fully enforceable on 1 June 2022. A Personal Data Protection Committee (**PDPC**), which is the regulatory authority, has been officially formed and several subordinate laws have been enacted. This overview of Thailand's privacy and data protection laws is based on the PDPA.

Thailand also has sector-specific laws and guidance that contain data protection related obligations, including laws for telecommunications, banking and e-payment, public health, government agencies, etc.

REGULATOR / AUTHORITY

The PDPC has been established to supervise compliance with the PDPA, under the supervision of the Minister of Digital Economy and Society (**MDES**).

The PDPC will appoint one or more Expert Committees (based on their field of expertise) to assist the PDPC with considering complaints under the PDPA, investigating acts of data controllers / data processors, settling disputes in relation to personal data and any other act assigned by the PDPC. At the time of this publication, Expert Committees have yet to be appointed.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

A DPO must be appointed where:

a. the data controller or the data processor is a public authority as prescribed and announced by the PDPC;

b. the data controller or the data processor requires regular monitoring of personal data or systems due to the collection, use or disclosure of large amounts of personal data as prescribed and announced by the PDPC. At present, the PDPC has not issued any rules or regulations on this matter; or

c. the core activity of the data controller or the data processor involves the collection, use, or disclosure of sensitive personal data.

The DPO must advise the data controller or the data processor, including employees or service providers of the data controller or data processor, on their PDPA duties and obligations. The DPO must also inspect operations to ensure compliance and cooperate with the PDPC on any PDPA compliance issues relating to the organisation. It's essential that the DPO maintains the confidentiality of the personal data accessed or acquired while performing their duties under the PDPA.

The data controller and data processor must provide the DPO's details, including contact address and contact channels, to the data subject and the PDPC. At present, there are no clear criteria or timeframes for providing DPO details to the PDPC, but the data controller and the data processor should do so in a timely manner.

The law does not impose any specific requirements for the DPO's location or residence. Organisations may outsource or subcontract the DPO function to third parties as long as that does not interfere with or conflict with the DPO's performance of their duties under the PDPA.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The PDPA applies to a person or legal person that collects, uses, or discloses the personal data of a natural (and alive) person, with certain exceptions (e.g. exception of household activity). "Personal data" is defined under the PDPA as "any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased person in particular".

Sensitive personal data is not specifically defined in the PDPA. However, it is understood to encompass personal data revealing racial or ethnic origin, political opinions, religious or philosophical belief, trade union information, health and medical information including disabilities, genetic or biometric data, a natural person's sex life or sexual orientation, an individual's criminal record, and any data which affects the individual in the same manner as prescribed by the PDPC.

Any collection, use, and / or disclosure of personal data by a data controller or processor that is in Thailand is caught under the PDPA, regardless of whether such collection, use, or disclosure actually occurs in Thailand or not.

The PDPA has extra-territorial applicability over foreign data controllers or processors that collect, use, and / or disclose personal data of individuals who are in Thailand where the activities of collection, use, and disclosure are related to:

- the offering of goods or services to the individuals who are in Thailand, irrespective of whether the payment is made by the individual; or
- the monitoring of the individual's behaviour, where the behaviour takes place in Thailand.

EMPLOYEE DATA / INFORMATION

Employee data is protected under the PDPA, in the same way as personal data. As there are no specific rules or regulations on collecting and processing an employee's personal data, it must be treated uniformly under the PDPA.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

The data controller may not use, disclose or transfer an individual's data without consent unless it has been exempted from the consent requirement (i.e. on the grounds of other legal bases of processing). The data must not be disclosed on any other basis except the purpose for which it was acquired. As mentioned below, individuals also have the right to object to the transfer of their personal data overseas under certain circumstances.

Personal data must not be transferred outside of Thailand, unless the recipient country or international organisation has adequate personal data protection standards in the PDPC view (e.g. EU GDPR) and the transfer is in accordance with the rules prescribed by the PDPC. The PDPC is currently considering a rule for data transfer of personal data to overseas jurisdictions, however, the rule has yet to be enacted and no further timing for enactment has been provided.

There are some limited exceptions to the cross-border transfer requirements, for example where:

- the individual has given consent and proper notification has been given by the data controller;
- the transfer is necessary for the performance of a contract between the data controller and the individual; or
- the transfer is necessary in order to protect the vital interests of the individual.

Transfers of personal data between group organisations may be exempt from the above requirement if the international transfer is to an organisation within the same group / affiliated business and such transfer is for joint business operations and there is a personal data protection policy that has been put in place and such policy has been reviewed and certified by the PDPC.

It is believed that the PDPC has the power to announce certain jurisdictions or countries to be "whitelisted", specifically those that have an "adequate data protection standard". However, this will need to be clarified when further guidance and sub-regulation is established.

Additional protective measures for cross-border transfers

There are no requisite measures that organisations must take when processing a cross-border transfer. But the PDPA states that personal data may be transferred to a foreign jurisdiction if the data controller and the data processor can provide "suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures according to the rules and methods as prescribed and announced by the PDPC".

Currently, there are no such approvals on security measures for cross-border transfers available.

Data sovereignty / localisation

Outside of the above cross-border transfer restrictions, there are no specific data sovereignty or localisation requirements (such as governmental consent, approval, or registration requirements) under the PDPA.

The PDPA does not require any registration of data controllers, data processors or data processing activities. This may change when subordinate laws are enacted. However, there is currently a requirement to prepare and maintain records of personal data processing activities in order to enable individuals to whom the personal data belongs and the PDPC to check upon.

COLLECTION AND PROCESSING OBLIGATIONS

Before an organisation can collect personal information, it must notify the individual of:

- the purpose of processing their personal data;
- whether the collection is a statutory or contractual requirement and the consequences of the failure of an individual to provide such data;
- the retention period to which their personal data will be stored;
- the organisations or third parties to which their personal data may be disclosed;
- the organisation's identity and contact details (or the details for the company that collects the personal data); and
- their individual rights.

The legal bases for collecting and processing general personal data are:

- consent;
- the achievement of the purpose relating to the preparation of the historical documents or the archives for public interest, or for purposes relating to research or statistics;
- the prevention or suppression of a danger to the individual's life, body, or health;
- when necessary for the contract with the individual, or in order to take steps at the request of the individual prior to entering into a contract;
- in the public's interest;
- legitimate interests of the data controller, another person, or organisation, except where such interests are overridden by the fundamental rights of the individual of his or her personal data; and
- necessary to comply with other legal obligations.

The legal bases for the collection and processing of sensitive personal data are:

- explicit consent;
- the prevention or suppression of danger to the individual's life, body, or health when the individual is incapable of consenting;
- when foundations, associations, or non-profit bodies carry out legitimate activities with appropriate safeguards for their members or associated individuals and do not disclose the sensitive personal data outside of their organisation;
- when sensitive personal data has been made public with the individual's explicit consent;
- when necessary for the establishment, compliance, exercise, or defence of legal claims; and
- when necessary to comply with a law for the purpose of:
  - preventive medicine or occupational media, the assessment of working capacity of the employee, medical diagnosis, health or social care, medical treatment, the management of health or social care systems and services;
  - public interest in public health;
  - employment protection, social security, national health security, social health welfare, the road accident victims protection, or social protection;
  - scientific, historical, or statistic research purposes, or other public interests; and
  - substantial public interest.

SECURITY REQUIREMENTS

Organisations that control personal data must implement appropriate security measures to prevent the loss, unauthorised access, use, alteration, or disclosure of personal data. These measures must be reviewed on a regular basis to ensure relevancy. These organisations are also liable for any third party (e.g. processors) use or disclosure of personal data in its control.

At the time of this publication, the PDPC has only announced rules and methods relating to the data controller's security measures. These were issued in 2022. Data controllers must also maintain records of personal data processing activities, which must include an explanation of security measures. They must be able to produce these records for inspection by an individual or the PDPC on request.

Data minimisation

The PDPA requires compliance with the principle of data minimisation in that the collection of personal data should be limited to the extent that is necessary for the lawful purpose of the data controller. In addition, the data controller shall ensure that the personal data remains accurate, up-to-date, complete, and not misleading.

If any personal data is no longer necessary or relevant, the data controller must delete, destroy, anonymise, or dispose of this data. However, the data controller can retain and process the personal data under circumstances when the data controller has a legal obligation or right to do so. Examples are:

- freedom of information;
- public interest;
- the purpose of establishment, compliance or exercise of legal claims;
- defence of legal claims; and
- the purpose for compliance with the law.

BREACH NOTIFICATION

The data controller is required to notify the PDPC of the personal data breach without delay and, where feasible, within 72 hours after having become aware of the breach.

If the personal data breach is likely to result in a high risk to the rights and freedoms of the persons, the data controller is required to notify individuals of the breach incident and the remedial measures without undue delay. The exemptions will be prescribed further in the sub-regulation.

The data processor is required to notify the data controller of the personal data breach that occurred.

INDIVIDUAL RIGHTS AND ACTION

Right to access

Individuals have the right to access or obtain copies of personal data about them that was collected, used, disclosed and / or transferred overseas by the data controller, or to request the data controller to disclose the source of the personal data that was collected without the data subject's consent.

Right to rectification

Individuals have the right to correct or rectify personal data held about them that the data controller collected, used, disclosed and / or transferred overseas when the personal data is incomplete, incorrect, misleading, or outdated.

Right to data portability

Individuals have the right to obtain personal data about them that the data controller retains in electronic format and in a clear structure. They can ask for this personal data to be transferred to another data controller unless the data controller cannot fulfill the request because of technical reasons.

Right to object

Individuals have the right to object to the collection, use, disclosure and / or cross-border transfer of their personal data under certain circumstances. These circumstances include:

- the collection, use, disclosure and / or transfer of personal data overseas for necessary actions — unless the data controller can demonstrate a more valid legitimate interest or that the collected personal data is processed to execute, exercise, or defend the data controller's legal claims; and
- any collection, use, disclosure and / or overseas transfer for direct marketing purposes.

Right to restriction

Individuals have the right to restrict or suspend the use of their personal data. This includes when the collected personal data is being verified to check:

- its integrity, relevance and completeness
- whether the data is misleading
- whether the data should be deleted or destroyed for unlawfulness
- whether the data still needs to be retained.

Right to withdraw consent

Individuals have the right to withdraw their consent for collecting, using, disclosing and / or transferring their personal data overseas at any time for the purpose the consent was given.

Right to erasure

An individual can ask the controller to erase, destroy or anonymise their personal data when consent is withdrawn or when the personal data is no longer needed for the purposes of the collection, use, or disclosure of personal data.

Individuals have an overall right to restrict the use of their personal data in certain circumstances (e.g. when it is no longer necessary to retain such personal data, but the individual requests the retention for the establishment, compliance, or exercise of legal claims, or the defence of legal claims).

Direct right of action / right to complain

Individuals do not currently have a "direct right of action" for a breach or interference of privacy in Thailand. However, individuals may file complaints with the PDPC and claim compensation for any damage caused by violating their personal data.

Pursuant to the regulation of the PDPC regarding the submission, refusal, termination, consideration and period for considering the complaints B.E. 2565 (2023), the PDPC must complete the preliminary examination of the complaint within 15 days from the date that a complaint receipt has been issued. After that, the Expert Committee will finish its consideration of complaint within 90 days of the first meeting. This period can be extended twice, for up to 60 days each time.

The court has the power to order the data controller or the personal data processor to pay punitive damages of up to two times the actual compensation.

PRIVACY BY DESIGN AND DEFAULT

The PDPA does not refer specifically to the concept of "privacy by design and default" but it was fashioned in close alignment with the GDPR, which adopts those concepts.

ENFORCEMENT

The PDPC can consider complaints made under the PDPA and investigate alleged breaches of the PDPA. It will mediate disputes and can issue notifications or orders pursuant to the PDPA. The PDPC has the right to enforce the law and impose penalties, where required.

Moreover, the PDPC can also announce and establish rules / guidelines for data controllers and personal data processors to follow and comply with.

Penalties / fines

There are three types of penalties under the PDPA — civil, criminal, and administrative penalties.

Failure to comply with the PDPA could result in civil liabilities with punitive damages (limited to twice the amount of actual compensation), administrative fines of up to THB 5 million, and criminal penalties which include imprisonment for up to one year, or a fine of up to THB 1 million (approx. EUR 26,600), or both.

The director, manager or the responsible person of an organisation may also be criminally liable under the PDPA if the relevant offence(s) resulted from that person's order, action, or omission.

As there are no precedent cases as yet, it is unclear how the PDPC will enforce its rights in actuality.

Consequences for breaches of data sovereignty / data localisation requirements

There are no specific penalties applicable to breaches / non-compliance data sovereignty / data localisation requirements.

Directors' duties

There are no specific directors' duties that apply under the PDPA. But directors can be held liable for breaches of the PDPA if they happen as a result of their instructions or acts.

UPCOMING REFORM

There are no proposed reforms or amendments currently in place in relation to the PDPA. However, there may be release of some notifications / guidelines released by the PDPC that will help with interpretation of the PDPA.

VIETNAM

KEY PRIVACY / DATA PROTECTION LAWS

As of 1 July 2023, the Decree on Personal Data Protection (**PDPD**) came into effect and is Vietnam's first comprehensive personal data protection law. It aims to protect the personal data rights, prevent personal data breaches and raise the awareness of relevant agencies, organisations, individuals when processing personal data. The PDPD generally applies to:

- Vietnamese and foreign agencies, organisations and individuals (including those operating abroad); and
- foreign agencies, organisations and individuals in Vietnam, or who are directly involved in or involved in personal data processing activities in Vietnam.

Constitutional rights

Prior to the PDPD, there were various Vietnamese legal instruments that touched on the protection of personal data and typically industry-sector specific.

Under the *Constitution of the Socialist Republic of Vietnam,* every person is entitled to the inviolability of personal privacy, personal secrecy and familial secrecy and has the right to protect his or her honour and prestige. Any information regarding personal privacy, personal secrecy and familial secrecy is safely protected by the law.

Cybersecurity law

In addition, from a cybersecurity perspective, *Law No. 24/2018/QH14 on Cybersecurity* (**Cybersecurity Law**). The Cybersecurity Law is less concerned with individual protections and was implemented to allow the Vietnamese government to monitor and control the flow of information and for the protection of information systems that are critical to national security.

Decree on Personal Data Protection

A major development for the protection of personal data occurred on 17 April 2023, when the Vietnamese government issued the PDPD. The PDPD came into effect on 1 July 2023, which consists of 44 Articles, divided into four Sections as follows:

- **Section I** — covering the scope of application; subjects of application; definitions; personal data protection principles; the handling violations of personal data protection regulations; State management on personal data protection; application of the PDPD, relevant laws and international treaties; international cooperation on personal data protection; and prohibited conduct.
- **Section II** — covering the rights and obligations of the data subjects; personal data protection when processing personal data; impact assessment and cross-border personal data transfer; measures, conditions to ensure personal data protection.
- **Section III** — covering the responsibilities of the Ministry of Public Security (MPS), Ministry of Information and Communications (MIC), Ministry of Science and Technology (MST), other ministries, ministerial-level agencies and agencies attached to the government, the data controller, data processor, data controller cum processor, third party and other relevant parties.
- **Section IV** — which covers enforcement validity and enforcement responsibilities.

As at the time of this publication, the PDPD is the main data protection law in Vietnam and therefore will be the focus of this guide.

Definition of personal information

The PDPD defines 'personal data' as *information (in the form of symbols, scripts, notebooks, images, sounds or similar forms in the electronic environment) which is attached to a specific person or helps to identify a specific person. Personal data includes basic personal data and sensitive personal data.*

Specifically:

- Information that helps identify a specific person is information formed from the activities of a person that, when combined with other data and information, can identify a specific person.
- 'Basic personal data' includes:
    a. Full name, middle name and birth name, other names (if applicable);
    b. Date, month and year of birth; date, month, death or disappearance;
    c. Gender;
    d. Place of birth, place of birth registration, permanent residence, temporary residence, current residence, hometown and contact address;
    e. Nationality;
    f. Photographs of the individual;
    g. Phone number, identity card number, personal identification number, passport number, driver's license number, license plate number, personal tax identification book, social insurance number, health insurance card number;
    h. Marital status;
    i. Information on family relationships (parents, children);
    j. Information on personal accounts; personal data reflecting activities and history of activities in cyberspace;
    k. Other information attached to a specific person, or which helps to identify a specific person that is not sensitive personal data.

- The PDPD provides a non-exhaustive list of 'sensitive personal data', including:
    a. Political and religious views;
    b. Health status and private life recorded in medical records, excluding information on blood type; information related to ethnic background and ethnic origin;
    c. Information on inherited or acquired genetic characteristics of the individual;
    d. Information on the individual's own physical attributes and biological characteristics;
    e. Information on the individual's sexual life and sexual orientation;
    f. Data on crimes and offences collected and stored by law enforcement agencies;
    g. Customer information of credit institutions, foreign bank branches, intermediary payment service providers and other permitted organisations (including customer identification information as prescribed by law, information on accounts, information on deposits, information on deposited assets, etc., information on transactions, information on organisations and individuals who are guarantors at credit institutions, bank branches, intermediary payment service providers);

h. Data on the location of individuals determined through location services; and

i. Other personal data specifically prescribed by law and requires necessary security measures.

REGULATOR / AUTHORITY

Under the PDPD, the MPS is the main body who is responsible for management and enforcement of personal data protection in Vietnam.

1. Ministry of Public Security

Some of the MPS's functions or powers are to:

- Assist the government in performing unified state management of personal data protection.
- Guide and implement personal data protection activities, protect the rights of data subjects against violations of the law on personal data protection, propose the promulgation of personal data protection standards and application recommendations.
- Develop, manage and operate the national portal on personal data protection.
- Evaluate the results of personal data protection work of relevant agencies, organisations and individuals.
- Receive dossiers, forms and information on personal data protection as prescribed under the PDPD.
- Promote measures and conduct research to innovate in the field of personal data protection and implement international cooperation on personal data protection.
- Inspect, examine, settle complaints, organise and handle violations of regulations on personal data protection in accordance with the provisions of law.

The specialised agency for personal data protection is the Department of Cyber Security and High-Tech Crime Prevention and Control — MPS, which assists MPS in performing the state management of personal data protection.

In addition to the MPS, there are other following competent authorities which jointly manage and regulate the personal data protection in Vietnam.

2. Government

The government uniformly manages the state for the protection of personal data.

Responsibilities of the state management of personal data protection include:

- To submit to competent state agencies for promulgation or promulgate according to their competence legal documents and direct and organise the implementation of legal documents on personal data protection.
- Formulate and organise the implementation of strategies, policies, schemes, projects, programs and plans on personal data protection.
- To gradually guide agencies, organisations and individuals on personal data protection measures, processes and standards in accordance with the provisions of the law.
- Propagate and educate the law on the protection of personal data; communication, dissemination of knowledge and skills to protect personal data.
- Develop, train and retrain cadres, civil servants, public employees and persons assigned to personal data protection.

- To inspect and examine the observance of the provisions of the law on personal data protection; settle complaints and denunciations and handle violations of the law on personal data protection in accordance with the provisions of the law.
- Statistics, information and solicitations on the situation of personal data protection and the implementation of the law on personal data protection for competent state agencies.
- International cooperation on personal data protection.

3. Ministry of Information and Communications

Some of the functions or powers of the MIC are to:

- Direct the media, press, officials and enterprises in the field of inquiry to protect personal data in accordance with PDPD.
- Develop, guide and implement measures to protect personal data and ensure cyberinformation security for personal data in information and communication activities according to assigned functions and tasks.
- Cooperate with the MPS in inspecting, examining and handling violations of the law on personal data protection.

4. Ministry of Defence

Responsibilities of the Ministry of Defence include managing, inspecting, examining, supervising, handling violations and applying personal data protection regulations to agencies, organisations and individuals which is under the management of the Ministry of Defence in accordance with the provisions of law and assigned functions and tasks.

5. Ministry of Science and Technology

Some of the functions or powers of the MST are to:

- Coordinate with MPS in formulating personal data protection standards and recommendations for application of personal data protection standards.
- Research and discuss with MPS on measures to protect data to keep pace with the development of science and technology.

6. Other ministries, ministerial-level agencies and agencies attached to the government

More broadly, state management authorities for particular industry sectors may also play a role in protecting information systems relevant to organisations operating in the industry sector that they oversee / regulate.

Some of their functions or powers are to:

- Perform the state management of personal data protection for management sectors and fields in accordance with the law on personal data protection.
- Formulate and implement contents and tasks of personal data protection in PDPD.
- Supplement regulations on the protection of personal data in the construction and implementation of tasks of ministries and branches.

- Allocate funds for personal data protection activities according to the current budget management decentralisation.
- Promulgate an open data catalogue in accordance with regulations on personal data protection.

For example, the State Bank of Vietnam oversees information security in bank operations and the Ministry of Industry and Trade oversees information relating to the security of consumer's rights and the protection of personal data in the e-commerce sector.

7. Provincial People's Committees

Some of their functions or powers are to:

- Perform the state management of personal data protection for branches and fields of management in accordance with the law on personal data protection.
- Implement the provisions on personal data protection in PDPD.
- Allocate funds for personal data protection activities according to the current budget management decentralisation.
- Promulgate an open data catalogue in accordance with personal data protection regulations.

DATA PROTECTION OFFICER (DPO) REQUIREMENT

The PDPD requires companies that process sensitive personal data to appoint a DPO and DPD, who will ensure the organisations comply with the PDPD. The details of the DPO and DPD must be communicated to the MPS.

The PDPD does not set out specific requirements on the criteria and qualifications of the DPO and DPD to be appointed. However, from a practical point of view, it is recommended that the DPO and DPD be based in Vietnam to allow for ease of communication with the MPS. Micro, small, medium and start-up enterprises (except for enterprises directly engage in personal data processing business activities) are given a grace period of 2 years from their establishment to comply with the provisions on designation of DPO and DPD.

SCOPE AND EXTRA-TERRITORIAL APPLICATION

The PDPD applies to the following subjects:

- Vietnamese agencies, organisations and individuals;
- foreign agencies, organisations and individuals in Vietnam;
- Vietnamese agencies, organisations and individuals operating abroad; and
- foreign agencies, organisations and individuals directly involved in or involved in personal data processing activities in Vietnam.

The term "personal data processing" means one or more activities affecting personal data, such as: collecting, recording, analysing, confirming, storing, editing, publicising, combining, accessing, retrieving, revoking, encrypting, decoding, copying, sharing, transmitting, supplying, transferring, deleting, and destruction of personal data or other related actions.

EMPLOYEE DATA / INFORMATION

Under the PDPD, personal data refers to personal data of all individuals (including employees).

All personal data processing activities of employees are therefore subject to the regulations of the PDPD.

CROSS-BORDER TRANSFERS AND DATA SOVEREIGNTY

Cross-border transfers

Under the PDPD, cross-border data transfer means the use of cyberspace, devices, electronic means, or other means of transferring personal data of Vietnamese citizens to a location outside of Vietnam or using a location outside of Vietnam to process personal data of Vietnamese citizens, including:

a. Organisations, enterprises and individuals transfer of the personal data of Vietnamese citizens to overseas organisations, enterprises and management departments for processing in accordance with the purposes agreed to by the data subjects; and

b. Processing personal data of Vietnamese citizens by automated systems located outside of Vietnam in accordance with the purpose agreed to by the data subjects.

The transferor of personal data must prepare and send an original copy of the cross-border personal data transfer impact assessment form in accordance with a standard form provided in the PDPD and other supporting documents (**TIA Dossier**) to the Department of Cybersecurity and High-Tech Crime Prevention and Control under MPS within 60 days from the date of processing personal data. The dossier must be available at all times to serve inspection and assessment by the MPS, and any changes to the content of the dossier must be updated/supplemented accordingly within 10 days of such changes. TIA Dossier includes key details such as contact details of the data transferor and recipient, objectives of the personal data processing after transfer overseas, types of personal data to be transferred and measures for personal data protection, among others.

The MPS can request amendment of the TIA Dossier, as well as to cease the cross-border transfers of personal data if (i) the data is used for activities that violate the interests and national security of Vietnam; (ii) the transferor fails to complete or update the TIA Dossier; or (iii) a Vietnamese citizen's personal data is leaked or lost.

Upon the completion of the data transfer, the transferor of personal data must notify the MPS in writing with information about the data transfer and contact details of the organisations, individuals in charge.

Data sovereignty / localisation

The Cybersecurity Law requires domestic and foreign enterprises to store personal data in Vietnam where the organisations both:

a. provides services over a telecommunications network or the internet, or value-added services on the internet in Vietnam; and

b. collects, exploits, analyses, and processes personal data or data regarding the user's relationship, or other data created by users located within Vietnam.

Foreign enterprises subject to this requirement must establish their presence in Vietnam (i.e., branch or representative office).

Impact assessment on personal data processing

Any personal data processing activity is also subject to the personal data processing impact assessment (**PDPIA Dossier**). This is a mandatory dossier for any entity that processes data, including for the cross-border transfer of data. This means that any entity that intends to transfer data overseas will need to complete both a TIA Dossier and a PDPIA Dossier.

Accordingly, the dossier of personal data processing impact assessment must be prepared in accordance with a standard form provided in the PDPD and other supporting documents and submitted to the Department of Cybersecurity and High-Tech Crime Prevention and Control under MPS within 60 days from the date of processing personal data. The dossier must be available at all times to serve the inspection and assessment activities of MPS, any changes to the content of the dossier must be updated/supplemented.

COLLECTION AND PROCESSING OBLIGATIONS

Apart from the above-mentioned obligations, agencies, organisations, and individuals also may only process personal data after they have notified and obtained the consent of the data subjects.

Notification

The notification to data subjects must contain the following information:

a. the purpose(s) of data processing;

b. the types of personal data used for processing;

c. the methods of data processing;

d. other parties involved in the data processing;

e. potential consequences and damages that may occur from processing;

f. timeline of data processing; and

g. where personal data is processed for advertising and marketing purposes, the content, method, form, and frequency of product marketing.

The notification to the data subject must be given in a format that can be printed, copied in writing, including in electronic form or verifiable format.

Consent

Under the PDPD, consent must be made on a voluntary basis and based on the data subject's full understanding of the following:

a. the type of personal data to be processed;

b. the purpose of processing personal data;

c. the entities entitled to process personal data; and

d. the rights and obligations of data subjects.

Consent must be explicitly and specifically expressed in writing orally, or through other clear actions, such as ticking a consent box, sending a text message, or selecting consent in technical settings, or through other actions that demonstrate as such. Additionally, such consent must be expressed in a format that can be printed or reproduced in writing, including in electronic or verifiable format.

The consent of the data subject must be in accordance with the processing purpose. Where there are multiple purposes, each purpose must be listed separately to enable the data subject to consent to one or more of the listed purposes.

The data subject may give partial or conditional consent.

The consent of the data subject is valid until the data subject decides otherwise or the competent authority requests otherwise in writing.

In the event of a dispute, the responsibility for proving the data subject's consent rests with the data controller.

Through the authorisation in accordance with the provisions of the Civil Code, organisations and individuals shall carry out procedures related to the personal data processing of data subjects on behalf of the data subjects. In such cases, the data subjects must have clearly known and consent, unless otherwise provided by law.

Silence or non-response of the data subject is not considered consent.

SECURITY REQUIREMENTS

Personal data protection measures must be applied from when the personal data starts being processed and throughout the processing of personal data.

Organisations and individuals involved in the handling of personal information must take appropriate managerial and technical measures to protect the personal information that they collect and store and comply with technical standards and norms of network information security. Additionally, there are requirements to:

- formulate and promulgate regulations on personal data protection in accordance with the PDPD;
- conduct cybersecurity inspection for systems and devices and equipment serving the processing of personal data before processing; and
- irreversibly delete or destroy devices containing personal data in accordance with the PDPD.

As mentioned above, there is a requirement to appoint a DPO and DPD for sensitive personal data processing activities.

In the event or potential risk of a technical incident, organisations handling personal information are required to take remedial and / or blocking measures as soon as possible to mitigate any adverse effects to individuals.

Data minimisation

The data subject is entitled to request the organisations and individuals that process their personal data to delete the data in the following circumstances:

- the personal data is processed for purposes other than the purpose for which that the data subject has given consent;
- the data is no longer necessary for the purposes for which it was collected under their consent, and they accept any damage that may be caused by the deletion;
- data subject object the data processing and that such processing does not have a legitimate reason to continue;
- the processing of personal data is a violation of the provisions of law;
- the data subject withdraws consent; or
- deletion of the personal data is required by law,

unless retention of the personal data is otherwise required by other Vietnamese laws.

The deletion of data must take place within 72 hours after the request of the data subject, unless otherwise prescribed by law.

BREACH NOTIFICATION

After detecting a violation of any data protection regulation (not limited to the PDPD), the organisation and individual who are directly involved in or related to the personal data processing activities must notify the Department of Cyber Security and High-Tech Crime Prevention under MPS within 72 hours from the time the violation occurs in accordance with a standard form provided in the PDPD. A reason for the delay must be provided where notifications of the violation occur beyond the 72-hour timeframe.

The violation notification needs to include the following information:

a. description of the nature of the violation, including: time, place, behaviour, organisation, individual, types of personal data and quantity of relevant data;
b. contact details of employees assigned to data protection or organisations or individuals responsible for personal data protection;
c. description of possible consequences and damages caused by the violation; and
d. description of measures taken to address and minimise harms caused by the violation.

However, the notification can be made in batches and in stages to fully cover the notification contents required as specified above.

Any organisation or individual must notify the Department of Cyber Security and High-Tech Crime Prevention under MPS upon detecting the following cases:

- detecting violations of the law against the person's personal data;
- personal data is processed for wrong purposes, in contravention of the original agreement between the data subject and the data controller, the controller cum processor of personal data or violates the provisions of law;
- failure to protect the rights of data subjects or not being properly implemented; or
- other cases as prescribed by law.

Neither the PDPD nor any other regulation provides a timeframe in which the above notifications must be made.

Penalties / fines

Fines for data breach related contraventions vary depending on severity. Please see the Enforcement section below for further details.

INDIVIDUAL RIGHTS AND ACTION

Data subjects have various rights under the PDPD.

Right to be informed

The data subject has a right to be made aware of the processing of their personal data, unless otherwise provided by law.

Right of consent and right to withdraw consent

The data subject may or may not agree to allow the processing of his or her personal data, unless otherwise provided by law. Accordingly, data subjects may withdraw their consent to the processing of their personal data, unless otherwise provided by law.

Right to access

The data subject is entitled to access to view, correct or request correction of their personal data, unless otherwise provided by law.

Right to erasure

The data subject is entitled to delete or request the deletion of their personal data, unless otherwise provided for by law.

Right to restrict processing

The data subject is entitled to request to restrict the processing of his/her personal data, unless otherwise provided for by the law.

The restriction in processing data shall be made within 72 hours after the request of the data subject, with all personal data requested by the data subject to restrict, unless otherwise provided by law.

Right to obtain personal data

The data subject may request to provide themselves with their personal data, unless otherwise provided by law.

Right to object to data processing

The data subject is entitled to object the personal data processing in order to prevent or restrict the disclosure of personal data or use it for advertising or marketing purposes, unless otherwise provided for by law.

The requested parties shall comply with the data subject's request within 72 hours after receiving the request, unless otherwise provided by law.

Right to complain, denounce and initiate lawsuits

The data subject has the right to lodge complaints, denunciations or initiate lawsuits in accordance with the law.

Right to claim damages

The data subject has the right to claim damages in accordance with the law when a violation of personal data protection occurs, unless otherwise agreed by the parties or otherwise provided by law.

Right to self-protection

The data subject has the right to self-protection in accordance with the law, or request competent agencies and organisations to take measures to protect civil rights as prescribed in the Civil Code.

PRIVACY BY DESIGN AND DEFAULT

There is currently no specific requirement for organisations to embed "privacy by design/default" principles in the design of their services or products under Vietnamese law.

The PDPD requires organisations and individual to apply personal data protection organisational and technical measures from the time of commencement and throughout the processing of personal data.

ENFORCEMENT

Enforcement activities and applicable penalties will depend on the contravention or breach that has occurred and vary between the relevant Vietnamese supervisory authorities who have jurisdiction over the matter.

Contraventions or breaches of the Vietnamese law that may attract a fine include (among other things):

- failure to process a legitimate request from an individual or failure to notify them that a request has been processed;
- collecting personal information without consent;
- illegally collecting, using, publishing, and doing business with an individual's personal information;
- failing to promptly apply remedies or preventive measures to actual or threatened breaches; and
- disclosing personal information without consent.

Currently, the penalties related to non-compliance of personal data privacy are set out in Decree 15/2020/ND-CP dated 03 February 2020 (as amended by Decree 14/2022/ND-CP). Accordingly, non-compliance regarding security requirements (e.g., data processing or data sharing with third parties without consent, data use not aligned with primary purposes, etc.) or personal data minimisation above would fall into the monetary fine in a range from VND 2 million (approx. USD 90) to VND 70 million (approx. USD 3,060).

There is a draft Decree on administrative penalties for cybersecurity violations which might replace / supplement personal data non-compliance regulations in Decree 15/2020/ND-CP) (**Draft Decree**). Under the Draft Decree, both Vietnamese and foreign entities and individuals committing violations in cyberspace will be subject to administrative penalties including: a warning, monetary fines (e.g., up to 5% of revenue in the Vietnamese market of the previous fiscal year based on the violation's nature), additional penalties (e.g., revocation of operational licence / permit; prohibition of practising or doing work related to cybersecurity) and remedial measures depending on the nature and severity of the violation.

Criminal penalties may also be imposed for violations of rules governing confidentiality and safety concerning an individual's email, mail, telephone, or other forms of communications. Depending on the severity of the crime, penalties may include: a warning, a fine between VND 20 million (approx. USD 830) and VND 200 million (approx. USD 8,510), and / or non-custodial reform of up to three years or a prison sentence of between one and three years in duration.

Consequences for breaches of data sovereignty / data localisation requirements

As mentioned above, although there are yet specific penalties applicable to breaches or non-compliance of "data sovereignty / data localisation" requirements, if an organisation is in breach of its obligations with respect to cross-border transfers or personal data disclosures, it may be subject to financial penalties (which can range between VND 2 million (approx. USD 90) and VND 70 million (approx. USD 3,060) depending on the nature and seriousness of the breach).

Under the Draft Decree, organisations may be subject to an administrative fine up to VND 200 million (approx. USD 8,510) for failures to submit the PDPIA Dossier or TIA Dossier.

Directors' duties

There are no specific directors' duties imposed under the privacy and data protection laws of Vietnam.

However, there are general directors' duties under the Vietnamese enterprise law that may apply to data protection and security, including the duty to perform their delegated duties honestly, diligently to their best in the interests of the company and of shareholders of the company.

UPCOMING REFORM

As mentioned above, to ensure the enforcement of the regulations on cybersecurity and data protection, on 31 May 2023, MPS circulated a 3rd version of the Draft Decree for public consultation. Upon completion of the consultation, MPS will submit the final draft version to the government for further consideration and approval.

In brief, the Draft Decree governs administrative sanctions in relation to the five main areas: (i) information security; (ii) personal data protection; (iii) cyberattack prevention; (iv) implementation of cybersecurity protection activities; (v) prevention and protection acts against using cyberspace, information technology and electronic means to violate the law on social order and safety.

The Draft Decree introduces classes of penalties with monetary fines being the principal form of penalties. The fines can be applied in addition to, or in lieu of further sanctions or corrective actions. Accordingly:

- the additional sanctions will depend on the nature and severity of the violation and can take the form of suspension of operations or business licenses, confiscation of violating exhibits and expulsion from Vietnam; and
- the remedial actions include removal or modification of offending programs or software or products or equipment or its associated information or features, deletion or destruction of offending data, removal or rectification of distorted data, revocation of subscriber information or public apology.

This publication has been prepared by PricewaterhouseCoopers on behalf of Netskope. PwC does not accept any responsibility, duty or liability to any third party in connection with this publication or for the consequences of any of them using or relying on this publication, any such third party use or reliance on this publication is at their own risk. PwC makes no representation concerning the appropriateness of this publication for any third party.

This publication is for general purposes only and does not constitute accounting, financial, legal, tax or other professional advice and should not be used as a substitute for consultation with professional advisers.

This disclaimer applies:

- to the maximum extent permitted by law and, without limitation, to liability arising in negligence or under statute; and
- even if we consent to anyone other than Netskope receiving or using this publication.

Liability is limited by a scheme approved under Professional Standards Legislation.

PwC refers to the Australian member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see **www.pwc.com/structure** for further details.

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivaled visibility into any cloud, web, and private application activity. Thousands of customers trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.